Digital Citizen and Consumer Working Group

Report – August 2021

Submitted on behalf of DCCWG by co-chairs - Office of the Privacy Commissioner of Canada (OPC) and Office of the Australian Information Commissioner (OAIC)

Table of Contents

Executive Summary

Established in 2017, the Digital Citizen and Consumer Working Group (DCCWG) is focussed on considering the intersections of, and promoting regulatory co-operation between, the privacy, consumer protection and competition (also referred to as Anti-Trust) regulatory spheres. Our work goes to the heart of the Global Privacy Assembly's (GPA)[1] Policy Strategy to facilitate regulatory co-operation and collaboration to create 'a global regulatory environment with clear and consistently high standards of data protection'.[2] The DCCWG provides a forum that encourages dialogue, co-operation and the sharing of experiences regarding intersection issues. It further aims to advance how authorities from all three regulatory spheres may use existing frameworks, or foster new ones, to work together and secure superior data and consumer protection outcomes for society.

The DCCWG's work and mandate has never been more relevant. This is reflected in the growing focus on intersection issues taking shape in the form of new laws and regulations, policy initiatives, inquiries, and increased enforcement action by regulators across regulatory spheres. This intersection has often resulted in positive outcomes and, at other times, has presented new tensions. Data sits at the centre of our digital economy and does not conform to regulatory or geographical boundaries. It is clear further understanding and collaboration by authorities across these regulatory spheres is needed to achieve optimal regulatory outcomes across privacy, consumer protection and competition. In fact, as noted in this report and its appendices, we have seen that where such collaboration has taken place, there is the potential to accentuate where they are complementary, and mitigate tensions, such that each regulatory sphere's objectives are advanced.

There is growing interest in our work from data protection authorities, consumer protection and competition authorities, other public authorities, civil society and organisations. Our membership has expanded to 18 agencies, with the addition of four new members. Bringing a fresh perspective to intersection issues, the DCCWG also welcomed its third observer, the European Consumer Organisation, also known as the BEUC[3], to the Working Group. As regulators draw from learned experiences across these regulatory spheres, our Working Group continues to provide a forum for this important collaboration against the backdrop of an evolving technological landscape. Concurrently, DCCWG representatives continue to be widely sought after to speak at engagements that promote cross-regulatory collaboration and awareness of intersection issues. Such engagement forums include networks, conferences, academic forums, and professional association events.

The DCCWG's resolution adopted by the GPA membership in 2019 established a 2-year mandate

[1] It was then known as the International Conference of Data Protection and Privacy Commissioners (ICDPPC).

[2] Global Privacy Assembly, 'Strategic Plan 2019-2021', page 4-6. See: http://globalprivacyassembly.org/wp-content/uploads/2019/11/GPA-Strategic-Plan-2019-2021.pdf.

[3] An acronym derived from their French name, 'Bureau Européen des Unions de Consommateurs.'

for the DCCWG. As we conclude this mandate, this Annual Report presents an opportunity to provide an overview of our work. Looking ahead, the DCCWG are excited to build on our achievements and see merit and global demand to continue this important work as a permanent working group of the GPA.

We are pleased to present this report at the GPA's Closed Session 2021, and hope that members find our contributions useful.

Office of the Australian Information Commissioner	Office of the Privacy Commissioner, Canada
Co-chair	Co-chair

Introduction

The DCCWG studies the intersections between privacy and data protection, consumer protection and competition. The work is integral to the GPA and its Policy Strategy, supporting its strategic ambitions around leadership, regulatory co-operation and collaboration to create 'a global regulatory environment with clear and consistently high standards of data protection'.[4]

The Working Group was first established at the 39th *International Conference of Data Protection and Privacy Commissioners* (now the GPA) through the Resolution on Collaboration between Data Protection Authorities and Consumer Protection Authorities for Better Protection of Citizens and Consumers in the Digital Economy.

In 2019, the GPA adopted a resolution that refreshed the mandate of the Working Group to consider the interaction between the regulatory spheres of privacy/data protection regulation, consumer protection, and competition.[5] This resolution shaped the strategic direction of the Working Group to:

- **further our understanding** of the privacy and competition intersection;
- **continue to explore, understand and map regulatory intersections**, in particular, as it relates to developments across policy, legislation and enforcement activities;
- **sensitise authorities and networks** to regulatory intersection issues and promote cross-regulatory collaboration; and
- **identify, leverage, and build upon collaborative initiatives** and networks that consider intersection issues.

The purpose of this report is to inform the GPA of the work undertaken by the DCCWG over the 2021 year and outline future work of the Working Group, as it continues its exploration of the intersections between privacy, consumer protection and competition and looks towards other potential areas of regulatory intersectionality in the digital economy.

The DCCWG has regularly reported to the Strategic Direction Sub-Committee (SDSC) on the progression of its work through presentations at "Deep Dive" meetings and written quarterly reports. The DCCWG Co-chairs presented at the seventh meeting of the SDSC in May 2021. The DCCWG's presentations were well received by the SDSC, who recognised the DCCWG's strong contribution to achieving the regulatory co-operation objectives outlined in the GPA's Policy

[4] Global Privacy Assembly, 'Strategic Plan 2019-2021', page 4-6. See: http://globalprivacyassembly.org/wp-content/uploads/2019/11/GPA-Strategic-Plan-2019-2021.pdf.

[5] '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,' passed at the 41st International Conference of Data Protection and Privacy Commissioners. See: http://globalprivacyassembly.org/wp-content/uploads/2019/11/DCCWG-Resolution_ADOPTED.pdf.

Strategy. In particular, the DCCWG reported on the sensitisation work it has undertaken to bring the work of the DCCWG and the GPA to the attention of the outside world.

The current members and/or observers of the DCCWG are as follows:

- Office of the Australian Information Commissioner (co-chair)
- Office of the Privacy Commissioner of Canada (co-chair)
- Belgian Data Protection Authority, Belgium
- Datatilsynet, Denmark
- Datatilsynet, Norway
- European Data Protection Supervisor, Europe
- Federal Commissioner for Data Protection and Freedom of Information, Germany
- Federal Trade Commission, United States
- Information Commissioner's Office, United Kingdom
- National Privacy Commission, Philippines
- The Superintendence of Industry and Commerce, Colombia
- Commissioner of Personal Data Protection, Senegal (new member)
- National Commission for the Protection of Personal Data, Gabon (new member)
- State Inspector's Service of Georgia, Georgia (new member)
- National Institute for Transparency, Access to Information and Personal Data Protection (INAI), Mexico (new member)
- The European Consumer Organisation (BEUC) (new observer)
- Authority for Consumer & Markets, Netherlands (observer)
- The Personal Data Protection Commission, Singapore (observer)

Working Group Activities

The DCCWG's 2020/2021 Workplan sets out four workstreams:

1. Privacy and Competition 'Deep Dive'
2. Continued sensitisation and engagement in other fora
3. Tracking and facilitating actual cross-regulatory co-operation
4. Contribute to the GPA's Enforcement Co-operation Handbook

The second year of the DCCWG's current mandate has proved a success. Throughout 2021, the DCCWG has met its resolution commitments and objectives within its Workplan. This section of the report provides an overview of the work undertaken during the second year of our mandate.

1. *Privacy and Competition "Deep Dive"*

As part of our 2-year plan, we have set out to further our understanding of the intersections between privacy and competition. The DCCWG has accomplished this through the release of two complimentary reports – the DCCWG-authored '*Privacy and Data Protection as Factors in Competition Regulation: Surveying Competition Regulators to Improve Cross-Regulatory Collaboration'* and the commissioning of Professor Erika Douglas' independent academic report '*Digital Crossroads: The Intersection of Competition Law and Data Privacy'*.

Privacy and Data Protection as Factors in Competition Regulation

As noted in our 2020 Annual Report, the DCCWG previously set out to conduct a series of competition regulator interviews in order to gain further insights into this intersection. Having completed our interviews with twelve different competition authorities from around the globe, we distilled their views, practices and case studies into a report, entitled '*Privacy and Data Protection as Factors in Competition Regulation: Surveying Competition Regulators to Improve Cross-Regulatory Collaboration'*.

The Report sought to:

(i) understand how competition authorities are approaching privacy and data considerations when carrying out their anti-trust analyses, and

(ii) leverage the views and examples provided in advocating for greater collaboration between competition and privacy regulators.[6]

[6] In alignment with the mandate of the DCCWG to promote opportunities for cross-regulatory cooperation.

The report identifies key takeaways, areas of potential synchronicity between regulatory regimes as well as obstacles to be surmounted, and potential tensions to be mitigated.

The report highlights contemporary intersection issues including:

- data being shared as a competitive remedy,
- the potential of privacy regulation to facilitate anticompetitive conduct,
- the value in understanding each regulatory field's language, and
- how privacy and data are being perceived as competitive factors of competition analysis.

Perhaps most importantly, the report also includes multiple practical examples that illustrate how competition regulators have successfully incorporated privacy considerations into their enforcement work and through cross-regulatory collaboration or consideration, found the balance between the two without sacrificing the objectives of either in the process. The benefits of such collaboration are superior outcomes that holistically serve a robust digital economy along with individuals' privacy rights and consumer interests. The full *Privacy and Data Protection as Factors in Competition Regulation* report is attached as **Annex 1.**

Digital Crossroads

Where the above report surveys how competition agencies are considering privacy in their anti-trust analyses and where collaboration is occurring, its companion academic report helps shape and inform the base discussions and efforts underpinning that collaboration, and what further strategic directions it can take.

Commissioned by the DCCWG the independent academic review, written by Professor Erika Douglas, of Temple University Beasley School of Law, and entitled '*Digital Crossroads: The Intersection of Competition Law and Data Privacy*',[7] is the first report of its kind to delve comprehensively into the intersection between antitrust and data privacy. It provides a detailed overview of the current regulatory landscape, highlights complements and tensions between the philosophies at the centre of these two fields and underlines its emerging development as an important cross-regulatory challenge requiring further consensus-building and international collaboration.

As an independent academic report, Professor Douglas publicly released *Digital Crossroads* in July 2021. It was subsequently promoted through social media by Temple University (@TempleLaw) and the GPA to a combined audience of almost 14,000 followers. Further, the report has been shared with the Global Privacy Enforcement Network as well as members of the International Competition Network (ICN). In addition to being available for download through Professor Douglas'

[7] https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3880737.

SSRN[8] at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3880737, the full *Digital Crossroads* report is attached as **Annex 2.** In its short release time, a little more than one month before this Annual Report was submitted to the GPA Secretariat, *Digital Crossroads* has experienced a significant volume of global downloads and abstract views.[9]

2. Continued Sensitization and Engagement in Other Fora

The work of the DCCWG has garnered much global attention and interest, with Working Group members successfully increasing awareness of intersection issues and promoting cross-regulatory collaboration. Members of the DCCWG are regularly sought out to provide presentations, attend panels and give keynote addresses across a wide range of international networks and fora.

A snapshot of engagements in 2021:

- The Office of the Australian Information Commissioner (OAIC) participated in a panel discussion at the International Association of Privacy Professionals (IAPP) ANZ Summit 2021 on local and global developments that impact privacy, competition, consumer reform and regulation.
- The Office of the Privacy Commissioner of Canada (OPC Canada), the OAIC and the United States' Federal Trade Commission (US FTC) presented at the IAPP Global Privacy Summit 2021 on *Blurred Regulatory Lines*. The panel was moderated by Professor Erika Douglas, the DCCWG's commissioned academic with expertise in regulatory intersection issues in competition law and privacy.
- IAPP Canada also hosted a similar privacy/competition intersection panel to those above, involving a conversation between the Competition Bureau Canada and the OPC Canada, and highlighting an example of how privacy had been used (unsuccessfully) as an anti-trust defence in a Canadian Competition Tribunal case.
- The ICN held a privacy/competition panel involving an OPC Canada representative along with former US FTC Chair Timothy Muris, Australian Competition and Privacy law academic Dr. Katharine Kemp and Brazilian anti-trust lawyer Marcela Mattiuzo. The panel was moderated by France's *Autorité de la Concurrence*.
- The European Union's European Data Protection Supervisor (EDPS) and the OPC Canada participated in a panel at the Computer, Privacy and Data Protection Conference (CPDP), which considered the interplay between privacy, consumer protection and competition.

[8] Social Science Research Network.

[9] As of this Annual Report's submission to the GPA Secretariat, *Digital Crossroads* has been downloaded 357 times while the abstract has been viewed 1,262 times.

- The OAIC and OPC Canada presented the work of the DCCWG at the Asia Pacific Privacy Authorities 55th Forum.
    - At the Forum, the OAIC also presented on the Australian Consumer Data Right framework, which is a data portability framework built on strong privacy protections. In addition, the OAIC also presented on how the Consumer Data Right supports cross-border data flows, and raised how global interoperability in other data portability schemes could reduce regulatory burden and complexity for businesses.
- The Competition Bureau Canada, OPC Canada, and leading Canadian Privacy Lawyers participated in a Canadian Bar Association Webinar panel entitled *Happy Together: Privacy & Competition Law in a Digital Economy.*
- The UK Information Commissioner's Office (UK ICO), the US FTC and the EDPS participated in a Centre for Economic and Policy Research Competition Policy panel event where they discussed integrating anti-trust and privacy.
- The UK's Consumer Markets Authority ("CMA"), the UK ICO and Professor Erika Douglas participated in the Privacy Laws and Business virtual speaker series on a panel entitled *Collaboration and Collision: Competition, Consumer and Privacy Law.* The session was moderated by OPC Canada and represented the launch day of Prof. Douglas' *Digital Crossroads*.

Overall, the DCCWG has seen a growing interest and demand in public events that explore regulatory intersection issues between privacy and competition law from international privacy organisations and networks. This has led to increased awareness and sensitisation of intersection issues with key stakeholders and networks.

3. Tracking and Facilitating Actual Cross Regulatory Co-operation

This stream builds on previous work undertaken by the DCCWG. The DCCWG continues to identify examples of, and facilitate opportunities for, regulatory co-operation along a continuum from **informal** (such as engaging in Global Privacy Enforcement Network (GPEN) / International Consumer Protection Enforcement Network (ICPEN) workshops) to **more formal** actions (such as warning letters, co-ordination/collaboration on investigations, etc.)

The Working Group monitors individual regulator actions (regardless of which regulatory sphere they are responsible for) that demonstrate the intersections between regulatory regimes, and actual collaborative actions taken by regulators across all three regulatory domains (DCCWG Mapping of Regulatory Intersections and Actual Collaborative Actions Table). The DCCWG undertakes this work to enable members to learn more about regulatory intersection issues experienced by authorities across all spheres. This mapping table builds on work undertaken by the DCCWG since 2017 and is presented at **Annex 3.**

A snapshot of actual cooperative action undertaken worldwide and monitored by the Working Group:

- Members of the Working Group (the Columbian Superintendence of Industry and Commerce, the US FTC, the OPC Canada, the UK ICO and the OAIC attended the first ever joint GPEN / ICPEN Best Practices workshop, which brought together 175 privacy and consumer protection enforcement professionals to discuss substantive intersections and potential cooperation strategies between these regulatory spheres. Given the Working Group's experience with cross-regulatory work, we were invited to design and oversee the workshop's breakout sessions. The workshop involved participants considering a hypothetical scenario and discussing intersections, possible barriers and strategies to co-operation. This joint event itself represented a pragmatic example of cross-regulatory collaboration, which is a key objective of the Working Group.

- The UK ICO has joined forces with the UK's competition/consumer protection, communications and financial regulators in a 'Digital Regulation Cooperation Forum' (DRCF) to enhance cross-regulatory work and ensure efficient regulation across the digital landscape. The DRCF has planned its work for 2021/2022.

    - In line with their DRCF work, the UK ICO and the UK competition authority, the CMA, published a joint statement setting out their shared views on the relationship between competition and data protection in the digital economy. The statement affirms both authorities' commitment to working together to maximise regulatory coherence and to promote and support outcomes which are competitive, empower consumers through enhanced choice, transparency and service design, and safeguard individuals' rights to privacy. This simultaneously promotes competition and enhances data protection and privacy rights.

- Brazil's data protection agency, competition authority, national consumer protection authority, and Federal Prosecution Service issued a joint recommendation to WhatsApp and Facebook seeking that they postpone the introduction of its privacy policy, amid privacy, competition and consumer rights concerns.

- The EDPS has published two opinions on the European Commission's proposed Digital Markets Act and the Digital Services Act. The EDPS opinions provide the EU Commission with a range of considerations, and alternative drafting which seeks to ensure that there is no conflict with the GDPR. From the opinions, the EDPS recognised that competition, consumer protection and data protection law were three inextricably linked policy areas in the context of the online platform economy.

- Following findings from the Norwegian Consumer Council's 'Out of Control' report into the practices of the online advertising industry, the Norwegian Consumer Council filed formal complaints against Grindr's data practices to the Norwegian Datatilsynet, alleging a breach of the European Union's General Data Protection Regulation. The Norwegian Datatilsynet upheld the Consumer Council's complaint and issued an advance notice to Grindr of its intention to impose an administrative fine for disclosing data to third party advertisers without legal basis, and for disclosing special categories of data without valid exemption.

- Following international intervention by ICPEN members, also endorsed by members of the GPEN Committee, Google announced that app providers will be required to indicate on the Google Play Store what personal data each app keeps and potentially shares about its users. This was the first cross-regulatory enforcement action involving the privacy and consumer protection regulatory regimes.

4. Contribute to the GPA Enforcement Co-operation Handbook

The DCCWG has continued to coordinate the pending revisions to the GPA's Enforcement Co-operation Handbook (Handbook) with the GPA's Enforcement Co-operation Working Group (IEWG). As noted in the DCCWG's 2020 Annual Report, we contributed to the development of a high-level "co-operation" survey in relation to the Handbook. To elicit a wide array of responses, the Working Group approached select members of the ICN.

Looking ahead, the DCCWG will build on the relationships developed through the Deep Dive competition regulator interviews by asking select regulators to assist in the development of cross-regulatory collaboration case studies for inclusion in the revised Handbook.

The case studies the DCCWG aim to develop will focus on cooperation strategies between privacy and competition regulators, and the benefits competition regulators can derive from collaborating with their privacy counterparts. In light of the need for coordination across multiple working groups and across multiple regulators, the updated Handbook will be finalized in advance of the GPA's upcoming Closed Session.

Forward Looking Plan 2021-2022

In charting the future direction and upcoming mandate of the DCCWG, the Working Group has reflected on the focus of our work to date. As noted, given the continued and increasing relevance of its work, the DCCWG intends to seek "permanent Working Group status" under the GPA. Please see below for a general overview of the DCCWG's objectives since 2017, our accomplishments, and a Forward Work Plan which builds on previous work.

Note that our Forward Plan validates the continued relevance of these objectives, while evolving our focus to increase collaboration across all three regulatory spheres:

Objective	General Outputs and Forward Plan Activities
To **explore, map and better understand the growing intersection** of the regulatory spheres of privacy, consumer protection and competition	The DCCWG has advanced work under this objective in its work on the 2017-2018 White Paper, which focused on consumer protection; and during 2019-2021 in its work on the Deep Dive reviews on privacy/competition interplay. **The analytical complexity of the latter calls for further targeted reflection and development. In particular, it is planned that the DCCWG focus specifically on the broader implications of Mergers & Acquisitions to individual's privacy.**
To **sensitize authorities** across regulatory spheres to the intersection, such that a privacy authority recognizes a competition issue when they see it, and vice versa	The DCCWG has achieved significant success since its inception in sensitising key external stakeholders to intersection issues. There is a clear increase of interest and demand for DCCWG presentations and panels this year. **The DCCWG will continue to undertake this work, as an important ongoing activity, which contributes to the GPA's Strategic Priority of maximising the GPA's voice and influence.**
Identify collaboration strategies and tools where they exist, and advocate for and recommend them where they do not	This began at the Macao GPEN workshop, and will **remain a focus in the Forward Looking Plan, noting and learning from examples.**
Finally, to bring everything together and **encourage actual collaboration** across all three regulatory spheres	Facilitating actual collaboration across all three regulatory spheres goes to the heart of the GPA's Strategic Priorities to work towards a global regulatory environment with clear and consistently high standards of data protection, as digitisation continues at pace. With this in mind and considering the above, **this should represent an increased focus in our Forward Plan – facilitating collaboration.** Strategies include holding another cross-regulatory collaboration workshop, participation at ICN, a joint ICN/GPA event, and leveraging our additions to the GPA Enforcement Cooperation Handbook.

Environmental Scan of Other Regulatory Areas of Intersection with Privacy (Note: this will be a new objective of the DCCWG)	Consumer protection and competition laws and regulations are hugely impactful, but they are not the only regulatory spheres intersecting with privacy and data laws. Already, interplay issues in areas such as e-safety and telecom are presenting themselves as areas of potential study. **An environmental scan would identify, and ordinally assess other regulatory spheres according to risks, opportunities and potential impact on the digital society and economy.**

Conclusion

At the centre of the DCCWG's work is a recognition of the importance of regulatory co-operation in the protection of personal information, particularly in an age of accelerated digitisation. The goal of the DCCWG, as reflected in our 2020-2021 Workplan, is to raise awareness and understanding of intersection issues between regulatory spheres and to promote regulatory co-operation between them. Such intersection issues will become more relevant as we respond to the challenges of the digital economy.

As part of our 2-year mandate, we committed to exploring the complements and tensions between the regulatory spheres of privacy and competition. The DCCWG is pleased with the insights generated from our privacy and competition "Deep Dive" as this has informed our understanding of the interaction between privacy and competition regulation and will guide and inform our members' further interaction and collaboration with competition authorities.

Our work has demonstrated that not only are traditional regulatory boundaries continuing to blur, but there exists substantial overlap between our regulatory domains. As regulators from all three backgrounds consider how to respond to this phenomenon, the need for regulatory cooperation among authorities to achieve holistic privacy and consumer outcomes is clear.

This is an area the DCCWG will continue to focus on and explore, as we hope to establish the Working Group as a permanent Working Group of the GPA. The extension of our mandate will ensure that we advance the Strategy Priority of the GPA to Advance Global Privacy in the Digital Age and continue to work towards a global regulatory environment with clear and consistently high standards of data protection.

The DCCWG co-chairs sincerely thank all members of the DCCWG for their valuable input and support to progress the mandate of the DCCWG and produce excellent practical outcomes for citizens and consumers. We look forward to our continued collaboration as we establish the DCCWG as a permanent Working Group to continue this important work.

Annex 1.

Privacy and Data Protection as Factors in Competition Regulation: Surveying Competition Regulators to Improve Cross-Regulatory Collaboration, by the DCCWG

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.

Annex 2.

Digital Crossroads: The Intersection of Competition Law and Data Privacy, by Professor Erika Douglas of Temple University Beasley School of Law

ACADEMIC REVIEW

DIGITAL CROSSROADS:

THE INTERSECTION OF COMPETITION LAW AND DATA PRIVACY

ERIKA M. DOUGLAS
Assistant Professor
Temple University, Beasley School of Law

REPORT TO THE GLOBAL PRIVACY ASSEMBLY DIGITAL CITIZEN AND CONSUMER WORKING GROUP

July 2021

Temple University
Beasley School of Law

Digital Crossroads: The Intersection of Competition Law and Data Privacy

Digital Crossroads: The Intersection of Competition Law and Data Privacy

This report was drafted with the dedicated research assistance of Heather Kemp, Megan Gehret, Christopher Perkes, Megan Young and Alex Park. Deepest thanks to the team at the Office of the Privacy Commissioner of Canada, Brent Homan, Adam Zimmerman and David Stenton for their commitment to review during the drafting process. All errors or omissions are the author's own.

Table of Contents

Table of Figures

Introduction

Antitrust and data privacy law are powerful forces shaping our economy. Scarcely a day goes by without headline-making enforcement from one regime or the other. The result is a wealth of new interactions between these areas of law—particularly in the digital economy.

This academic review, *Digital Crossroads: The Intersection of Competition Law and Data Privacy* (the Report) was written for the Global Privacy Assembly (GPA) Digital Citizen and Consumer Working Group. It seeks to identify and understand the interactions between antitrust and data privacy around the world, from the public perspectives of the agencies who enforce each area of law. The Report presents a typology describing the touchpoints between the two realms, based on analysis of the relevant law, objectives, policy, enforcement priorities and agency concerns.

As this Report describes, the interactions between antitrust and data privacy are nascent, varied and complex. Though often described simply as complementary, the relationship between antitrust law, competition itself and data privacy is often much more nuanced and multi-faceted. In some areas, like merger review, new theories are taking hold to address data privacy. In others, like antitrust remedies, there is only a nascent sense that the two realms may intersect. There remains significant room for development of theory and practice across this landscape of antitrust law and data privacy.

The goal of this Report is to deepen the shared understanding of antitrust and data privacy authorities regarding the many touchpoints between their domains. This is a rapidly evolving intersection of law with great significance to consumers. It demands attention and cooperation across agency bounds to develop cohesive, effective digital enforcement strategies. The hope is that this Report will contribute to cross-doctrinal understanding, and prompt agencies around the world to develop shared theories, collaboration and best practices at this new digital crossroads.

Executive Summary

This Report, written for the GPA Digital Citizen and Consumer Working Group, seeks to examine, describe and taxonomize the views of enforcement agencies on the intersection of data privacy and antitrust law.

As the length and breadth of this Report attests, we are entering an era of unprecedented interaction between antitrust and data privacy law. This intersection of law has expanded dramatically in recent years, as a result of:

- **The global expansion of data privacy law:** Today, approximately 130 jurisdictions have some form of data privacy or data protection legislation.[1] At least twenty others report that draft data privacy legislation is under consideration.[2] Several jurisdictions are amending and expanding their existing laws. This tidal wave of privacy law, and its enforcement, have brought about a new age of data privacy for consumers and businesses alike.

- **Renewed global attention to antitrust enforcement**: Antitrust law and policy have seen a global revival, with a flurry of attention to digital competition and a number of significant, new agency cases. Many of these antitrust cases are against large digital platforms—the same companies who often draw the attention of data privacy enforcers.

- **The shared focus of both legal regimes on the digital economy**: Interactions between antitrust and data privacy are the most stark, and the most common, in the digital economy. From online advertising, search and social media, to a myriad of location-based services, many digital businesses are driven by personal data processing. This has placed the digital economy front and center in data privacy enforcement. The size and economic importance of many digital platforms has made them a strategic priority for antitrust law. Whether framed as issues of digital markets, advertising, big data, zero-price products or otherwise, both antitrust and data privacy are occupying the same spaces in policy, law and enforcement.

[1] United Nations Conference on Trade and Dev. (UNCTAD), *Data Protection and Privacy Legislation Worldwide* (Feb. 4, 2020), https://unctad.org/page/data-protection-and-privacy-legislation-worldwide (noting 128 of 194 countries surveyed had some form of data privacy or protection legislation).

[2] *Id.* (full data reporting as of February 27, 2021).

These developments in law and the economy have produced a wealth of new interactions between antitrust and data privacy. Throughout the discussion, this Report emphasizes three broad themes that characterize this legal crossroads.

Report Themes: Understanding the Intersection of Antitrust Law and Data Privacy

1. **Antitrust and data privacy law are meeting in complex and multi-faceted ways, particularly in the digital economy.** Despite often being summarized as complementary or in tension, the relationship between antitrust law and data privacy is more nuanced. A closer examination reveals a landscape of multi-faceted interactions, many of which are only beginning to be recognized and understood.

2. **The theory and practice at this frontier of law are at an early stage.** Though the fact of interaction between antitrust and data privacy law is increasingly acknowledged, the theory and practice within this legal landscape remain quite new, and present significant opportunities for development.

3. **Data protection and antitrust authorities can no longer achieve their goals in isolation.** Antitrust and data privacy enforcers share many common policy interests, a focus on the digital economy and the ultimate goal of benefitting consumers. This rapidly evolving intersection of law demands cooperation across agency bounds to develop cohesive, effective enforcement strategies for the digital economy. As these legal realms increasingly interact, siloed enforcement of antitrust and data privacy law will undermine enforcers' shared interests, creating unnecessary or unintended gaps, overlap and tension between the two areas of law.

Research Methodology and Scope

- **The research for this Report included the review of more than 200 publicly available, English-language materials related to antitrust and data privacy agencies around the world.** The materials ranged from legislative objectives (in the agency's enabling legislation) to agency decisions, litigation filings, guidance, speeches, submissions, market/sector studies, and other relevant documentation from entities such as the Organization for Economic Co-operation and Development (OECD) and the GPA itself. The research focused on the jurisdictions that comprise the GPA Digital Citizen

and Consumer Working Group.

- **The Report excludes discussion of the interaction between consumer protection law and privacy law.** Though important and often related to the topic discussed here the intersection of consumer protection law and data privacy is addressed in an earlier report by the GPA Digital Citizen and Consumer Working Group.

- **The Report is relevant to enforcers in both antitrust and data privacy, but was drafted primarily for a privacy audience seeking to understand the potential relevance of antitrust law and policy to their work.**

Status of Collaboration Between Antitrust and Data Privacy Agencies

- **There is no single model of agency responsibility for antitrust law or data privacy law enforcement around the world.** In some jurisdictions, antitrust and data privacy law are enforced by separate regulatory authorities. In others, the same authority enforces both areas of law, and sometimes also consumer protection law.

- **Just a few years ago, the European Data Protection Supervisor voiced concerns over the "silo-ization" of antitrust and data privacy law enforcement,** and the increasing challenges such separation will pose for regulation of the digital economy.

- **Today, agency collaboration is growing rapidly in frequency and scope across the realms of antitrust and data privacy law. Authorities in several jurisdictions have taken action to develop or enhance collaboration across their spheres of responsibility**, including the following: recognizing that co-operation is matter of strategic importance, executing agency collaboration agreements, issuing joint guidance, co-operating on individual matters and developing structural efforts to build cross-doctrinal knowledge and best practices. Instances of such co-operation are summarized here, and tracked in further depth in an earlier GPA Digital Citizen and Consumer Working Group report.

Part I. Understanding Complementarity and Tension at the Roots of Antitrust and Data Privacy

Part I looks at the foundations of antitrust and data privacy law, which influence their interactions. It considers the legal framing of privacy rights and interests, why the two areas of law are interacting, the differences in the legislative objectives of each regime and the policy

interests shared by both.

- **Conceptions of "data privacy law" differ around the world.** As highlighted in this section and discussed throughout the Report, both privacy and antitrust law vary by jurisdiction. The interactions between the two areas of law will therefore vary as well.

    - In the European Union and its nation states, data privacy is a constitutionally protected right. In jurisdictions like the U.S., federal data privacy law is a sub-category of consumer protection law. In still others, like Australia and Canada, data privacy law is conceived of primarily in terms of principles, rather than rights or consumer protection. The legal roots of data privacy are evolving in some jurisdictions, with emerging rights conceptions in certain states and industries, and judicial recognition of the quasi-constitutional status of privacy.

    - These conceptual differences in the roots of data privacy law are likely to impact its interaction with antitrust law. Rights-based conceptions may strengthen the case for express consideration of privacy in competition analysis, and may also presents an "apples to oranges" reconciliation between privacy rights and the economic interests advanced by competition law. In jurisdictions like the U.S., where competition and privacy are both framed in economic terms, the analysis of tradeoffs between the two interests may become less complex, by virtue of their shared conceptual roots.

        - These differences in how privacy is conceived echo throughout the coverage of this Report. Agencies in the European Union have paid more extensive attention to the reconciliation of competition law and data privacy law, at least in part because such attention is demanded by the robustness of the General Data Protection Regulation (the GDPR) privacy rights and their corresponding relevance to data-driven competition.

    - This section adopts a working definition of "privacy law" for the purposes of the Report, based on how the concept is perceived at its point of intersection with antitrust law and policy. The definition narrows the focus to i) informational or data privacy as it relates to an individual's legally protected rights or interests to control the processing of their personal information and ii) the privacy obligations of non-governmental entities, as antitrust law is primarily concerned with the role of data in enterprise and competition, rather than the use of data by government.

- **At their highest level of abstraction, both data privacy and antitrust seek to benefit consumers. However, data privacy legislation and antitrust legislation set out different objectives, which reflect the distinct approaches of each realm to achieving consumer benefits.**

    - While data privacy law focuses on the protection of privacy interests of individuals, the main goal of modern antitrust law is to promote economic consumer welfare through competition. Antitrust law seeks to benefit consumers through a broad, economic efficiency prescription, in contrast to the individual rights or interests characteristically protected by privacy law.

    - Jurisdictions like the U.S., which focuses narrowly on the goal of economic efficiency, are more resistant to incorporating other considerations like privacy into antitrust analysis. The concern is that including privacy within competition analysis—particularly where privacy effects are unrelated to competition— may dilute or confuse the application of economic efficiency-based standards, making it unclear which factors should drive antitrust case or policy outcomes.

    - In addition to the main goal of economic consumer welfare, several jurisdictions also include distributional objectives in their competition legislation, such as fairness or the provision of equitable opportunities for businesses. Jurisdictions that pursue these broader antitrust goals may have greater scope for the inclusion of data privacy considerations antitrust analysis, relative to jurisdictions like the U.S. that hew strictly to the goal of economic consumer welfare.

- **Despite the distinct objectives of antitrust and data privacy law, agency materials clearly reflect several shared policy interests. Many of these shared interests relate to the digital economy.**

    - Both antitrust and data privacy enforcers seek to promote consumer trust in digital markets. Trust is viewed as a precursor to full economic participation, and its concomitant benefits for consumers.

    - Both legal regimes view data portability as beneficial, for privacy and for competition.

        - Jurisdictions around the world are granting and interpreting new data portability rights within their data protection laws.

        - These data portability rights have become one of the most emphasized areas of complementarity between data privacy law and competition policy. Data portability is thought to promote data-driven competition, by reducing barriers to consumer switching between services. This is thought to make it easier for new companies to obtain the supply of data necessary to enter or expand their products or services within a market.

        - Data portability rights are generally viewed as a positive for competition, but those rights may not necessarily be adequate to achieve robust competition in some markets. Several antitrust authorities have looked beyond data portability to more extensive models of data mobility, such as open standards or interoperability, as potentially necessary to restore competition. There have been notable antitrust initiatives to promote competition through interoperability in the banking sector.

    - Both legal regimes seek to encourage and maintain consumer choice in markets. There is a shared concern from both antitrust and data privacy authorities over phenomena that impact consumer choice, including consumer behavioral biases, information asymmetries and limited or complex product/service choice—particularly in digital products and services.

Part II. Theory and Practice at the Intersection of Antitrust and Data Privacy

Part II of the Report introduces the leading theory on the interaction between antitrust law and data privacy. It then delves into the practical application of this theory, and others, across several major topics of antitrust law: market definition and market power, merger review, abuse of dominance, cartels/competitor collaborations and remedies.

- **The leading theory on this intersection of law posits that antitrust analysis should consider data privacy when—and only when—privacy is a parameter of product (or service) quality that is affected by competition.** The Report refers to this as the "privacy-as-quality" theory.

    - For example, companies may compete to offer consumers more protective privacy features, or less collection and processing of personal data. Consider a merger between two internet browser companies who compete to offer users privacy-protective online features. The transaction might reduce the level of competition in the browser market to offer such features. If this reduction in competition is likely to cause a decline in privacy protection among browsers, the antitrust

assessment of the merger would account for that effect on privacy-related quality. The decline in privacy quality might include a degradation in the level of privacy protection afforded, or an increase in personal data processing without offsetting benefits.

- This theory could also apply where the anticompetitive conduct of a dominant firm causes a reduction in privacy-related competition and quality. The U.S. Department of Justice, Antitrust Division alleges this effect in a recent monopolization complaint against Google, arguing that "[b]y restricting competition in search, Google's conduct has harmed consumers by reducing the quality of search (including on dimensions such as privacy, data protection, and use of consumer data) . . . ."[3]

- Conversely, where a merger or misconduct is likely to have the effect of increasing privacy quality through competition, the antitrust law or policy assessment would view that effect as positive.

- **This "privacy-as-quality" theory is the most widely-articulated agency perspective on the relationship between data privacy and potential antitrust harm. However, its implications and potential applications are still at an early stage of understanding and development.** In theory, privacy could be considered an element of quality across many areas of antitrust law. In practice, as this Report explains, merger review has been the primary context for antitrust analysis of privacy-based competition, with some very early application in abuse of dominance cases.

- **This privacy-as-quality theory acts both to integrate and to limit the role of data privacy in antitrust analysis.**

  - **This theory incorporates data privacy into longstanding antitrust analytical frameworks,** which recognize that quality may be the basis for competition in some markets. It does so by interpreting the concept of "quality" as sufficiently broad to encompass the quality of privacy offerings in a market.

  - **Antitrust agencies also view this theory as a limit on their jurisdiction.** Where a merger or misconduct gives rise to privacy harms that are unrelated to competition—what might be termed "pure" privacy harms—multiple antitrust

[3] Press Release, U.S. Dep't of Justice, *Justice Department Sues Monopolist Google for Violating Antitrust Laws* (Oct. 20, 2020), https://www.justice.gov/opa/pr/justice-department-sues-monopolist-google-violating-antitrust-laws.

authorities have found that such harms are beyond their jurisdiction, and more appropriately matters for data protection law.

- **Although there is a growing acceptance of the privacy-as-quality theory among antitrust agencies, there are likely to be practical challenges in its application.** In particular, it may be difficult to precisely measure privacy-related effects on competition.

    - Established antitrust theories and models are primarily price-based. The measurement of non-price effects has long been recognized as a challenge for antitrust law—the likely difficulties in privacy quality analysis are simply the latest incarnation of this broader issue.

    - There are also specific factors that may make the measurement of privacy-related effects on competition more difficult, including: the often-heterogenous privacy preferences of consumers, the potential for tradeoffs between privacy and other parameters of product quality in the design of products and services (for example, increased online tracking in exchange for better-targeted behavioral advertising) and distortions in consumer privacy choice (such as behavioral biases).

    - Translating privacy or data effects into estimated monetary values does not necessarily solve such challenges in measuring privacy effects related to competition. At least one jurisdiction has described this data "price" equivalency analysis as deeply inconsistent with a rights-based view of data privacy.

    - Antitrust cases and investigations have used certain types of evidence to identify whether data privacy is the basis for competition, and the potential parameters for such competition. Though early-stage, this evidence includes: consumer and competitor surveys on whether data privacy is a driver of competition, observations of privacy-related market behavior (for example, whether competing companies change their privacy policies in response to one other) and internal company documents (for example, to provide insight on why a company made changes to its privacy policy). The OECD has also suggested that analysis of the amount and nature of personal data processing could be helpful in understanding privacy-related competition.

    - Despite these emerging sources of evidence, the difficulty remains that there are no settled analytical approaches, or even a clear set of potential options, for assessment of the magnitude or specific nature of privacy-based effects in antitrust analysis.

- **The lack of established, reliable analytical tools to evaluate competitive effects on privacy quality is likely to be a barrier to the integration of privacy considerations into antitrust analysis**.

- **This gap also presents a significant opportunity for collaboration between data privacy and antitrust authorities to develop reliable, well-founded methodology and tools for measuring competition-related effects on privacy quality**. In particular, the specialized expertise of data privacy authorities in measuring and evaluating privacy, and the effects of market conduct on privacy, could provide valuable insight to antitrust authorities seeking to evaluate privacy-based effects on competition.

A. Privacy, Market Definition and Market Power

- **Antitrust Law:** The starting point for antitrust analysis is often the definition of relevant antitrust markets, and an assessment of whether a firm holds market power within any of those markets.

- **Neither market definition nor market power analysis have focused expressly on privacy.** Instead, antitrust analysis has looked at the broader challenges posed by digital markets, including:

    - The various roles of data in driving (or limiting) competition and market power; and

    - "Zero-price" markets, which is a term used to refer to markets where the products or services have no monetary price, but require users to provide their data. Many digital markets involve zero-priced products. Since price cannot form the basis for competition in such markets, privacy and other aspects of product quality may take on a more prominent role in competition.

- **In considering digital markets, antitrust agencies have tended to reaffirm the resiliency, flexibility and applicability of existing analytical frameworks for market power and market definition.** At the same time, agencies acknowledge that such digital markets often share certain characteristics that present analytical challenges for antitrust law.

- **Modern market definition, particularly in merger reviews, tends to rely upon price-based methodologies.** This price-based analysis is ill-fitting for zero-price products or services, which do not charge consumers a monetary price.

    - Instead, multiple jurisdictions have considered whether the analysis might use a small but significant non-transitory decrease in quality test to define relevant antitrust markets. Discussion of such analysis often acknowledges that a quality-based test will be more difficult to operationalize than the standard, price-based analysis.

- **Antitrust authorities have paid extensive recent attention to two particular topics in the discussion of digital market power:**

    - **Whether and when data might confer market power or a competitive advantage.** This includes consideration of whether the scale and scope of data accumulation may act as a barrier to competition in certain markets. Where a firm accumulates data that is unique, and difficult for competitors to replicate in scale or type, this may create barriers to competitive entry and contribute to the firm's market power. However, in some markets competitors may be able to replicate the valuable data set themselves, or it may be that factors other than data accumulation (such as expertise in data analysis or use) create a competitive advantage. Market power must always be evaluated on a case-by-case basis in antitrust law.

    - **The role of network effects in market power.** Network effects are common in digital services, such as social networking or sharing ("gig") economy applications, where the larger the number of users, the more valuable the service becomes to other users. Antitrust authorities are interested in how network effects may amplify—or reduce—market power. Network effects tend to be described as bolstering the market power of incumbent firms, but may also play a beneficial role in promoting competition.

- **Market shares are often an important factor in the antitrust analysis of market power.** Revenue and profit measures tend to be a common basis for measuring market shares. In zero-price markets, however, different or additional measures of market share may be important, such as the number of users, or share of relevant interactions (such as views, searches or transactions). Ultimately, the appropriate market share measure will be highly specific to the market being considered, and often subject to debate.

- **Though antitrust law faces some challenges in the definition of zero-price markets and the estimation of market power in digital contexts, in practice, those challenges have not been so significant as to stymie antitrust enforcement.** Antitrust agencies have regularly defined markets, and concluded that market power is held by certain digital platforms that offer zero-price services.

B. Merger Review and Data Privacy

- **Antitrust Law:** Competition agencies around the world are empowered to review and challenge mergers (and other corporate transactions) that are likely to cause significant, negative effects on competition.

- **Antitrust agencies have considered the relevance of privacy-based competition to a greater extent in merger review than in other areas of antitrust law, though the interaction is still at the early stages of theory and practice.** As early as 2006-2007, the U.S. and EU antitrust authorities publicly began to contemplate the potential relevance of privacy-based competition in merger reviews. For example, in the high-profile acquisition by Google of Doubleclick in 2007, the U.S. Federal Trade Commission considered, but largely dismissed, concerns over the privacy effects of the merging parties combining their respective sets of advertising data.

- **There is emerging agreement among antitrust agencies that data privacy may be considered an element of quality-based competition in merger reviews.** There have now been a handful of mergers, primarily in the EU and U.S., where competition agencies have considered theories of competitive effects on privacy. These mergers involved markets for online advertising intermediation, consumer messaging applications and professional social networking services. Even in jurisdictions that have yet to consider a merger that raises this type of issue, there is often support in theory for the view that privacy may be a parameter of competition in certain markets.

- **However, from the *Google/Doubleclick* merger to present, both EU and U.S. antitrust agencies have made clear that they view any privacy concerns that are *unrelated* to competition as beyond their jurisdiction**.

    - For example, when Facebook acquired WhatsApp, a popular online messaging service, consumer privacy advocates pushed for antitrust agencies to block the merger. Their concern was that, post-transaction, Facebook would combine and use WhatsApp consumer data in a manner that violated WhatsApp's pre-merger

privacy policies. The European Commission considered these arguments, but concluded that "[a]ny privacy-related concerns flowing from the increased concentration of data within the control of Facebook as a result of the transaction do not fall with the scope of EU competition rules but within the scope of EU data protection rules."[4] The agency reached similar conclusions in response to privacy concerns that were raised when Google acquired FitBit, a company with large amounts of personal health and fitness data.

- **Only a small proportion of the mergers reviewed by antitrust agencies raise theories of privacy-related effects on competition. Among those mergers, even fewer have resulted in findings that such privacy effects are likely to occur.** This highlights an important distinction between mergers with data-related effects, which antitrust authorities regularly consider, and mergers with privacy-related effects, which are newer and relatively rare. The data involved in mergers is often not personal, and the competitive effects are often unrelated to privacy. The antitrust interests is the potential competitive effects that arise from the merger, regardless of whether the data involved is personal or not.

    - However, the European competition authorities have found that privacy quality was likely to decline in at least one transaction: Microsoft's acquisition of LinkedIn, a professional social networking company. Effects on privacy-based competition were likely to occur as a result of foreclosure of competing professional social networking services. The competing services offered stronger privacy protection to users than the merging parties, and post-merger, Microsoft would have the incentive and ability to exclude those competitors from the market. As a condition of merger approval, European competition authorities required Microsoft to agree to a number of conditions designed to ensure continued competition in professional social networking services.

- **Antitrust authorities often evaluate data-related merger effects that are not specific to personal data or privacy.** This includes consideration of:

    - Whether the accumulation or combination of data arising from a merger provides a competitive advantage, such as the creation of barriers to entry or expansion of competitors, increased market power, or increased potential for coordinated firm misconduct; and

[4] Eur. Comm'n, Facebook/WhatsApp, Case No. COMP/M.7217 C (2014) 7239, ¶ 164 (Oct. 3, 2014).

- Whether data is an input necessary for competition, and, if so, whether the merged parties would have the incentive and ability to limit or foreclose a rivals' access to that data post-merger.

- In assessing the likelihood of such data-related effects on competition, an important consideration is often whether the data at stake is unique, and exclusively within the control of the merging parties. Where data is replicable from other sources, several merger review decisions have concluded that negative effects on data competition are unlikely to occur.

- **Continuing cooperation between antitrust and data privacy agencies will be important in specific merger reviews and in the development of sound overall theories of merger-related privacy effects.** As the regulators with the deepest expertise on privacy, it is important that privacy agencies continue to contribute to the development of robust theories of merger-related effects. Recent mergers demonstrate that privacy agencies can offer valuable insight in specific cases regarding the likely effects of mergers on privacy-based competition and in the design of remedies that are positive for data privacy.

- **Though relatively few mergers impact privacy-based competition, it is possible that such mergers will become more common in the future, for several reasons.** Consumer demand for privacy protective products and services is rising, making privacy a more important parameter of competition in some markets. Antitrust enforcers are continuing to focus on data-driven transactions and effects in the digital economy. Finally, some jurisdictions are liberalizing their merger review laws to facilitate merger challenges, particularly in the digital economy. These developments have the potential to increase the number of merger reviews that involve personal data and privacy issues.

C. Abuse of Dominance and Data Privacy

- **Antitrust Law:** Most jurisdictions around the world prohibit abuse of dominance or "monopolization" in their competition laws. These laws vary by country, but the central focus is to prevent firms with market power from engaging in types of unilateral, anticompetitive conduct.

- **The relationship(s) between monopolization, competition and data privacy are not yet well-established or concretely understood.** Cases, investigations and policy views are beginning to assert a connection between the two, but it is too soon to identify

consensus thinking.

- When antitrust agencies refer to the connection between monopolization and privacy, the tendency has been to portray market power, or a lack of competition, as a likely cause of low privacy quality or choice for consumers.

- There has also been a less common suggestion that onerous privacy law may contribute to the entrenchment of existing monopolists, by making new entry of competitors more difficult.

- The research for this Report found little empirical evidence in agency materials that would support either view, or any potential alternative views, about the relationship between monopolization, competition and privacy.

- **Antitrust enforcement around the world is focused on abuse of dominance in the digital economy.** A 2020 International Competition Network survey found 30 of 39 respondent jurisdictions had opened abuse of dominance investigations in digital markets, and at least 17 were taking enforcement action.[5]

  - Theories of exclusion of competitors are by far the most common. However, there has also been a recent uptick in theories that allege exploitation of consumers or competitors, including a high-profile case brought by the German competition authority that alleges privacy exploitation. Both types of abuse are discussed in this Report.

  - Antitrust authorities have brought a small number of early-stage cases that allege dominance has been used to degrade available privacy protections and options for users of online social networking and online search.

  - However, most of the exclusionary antitrust cases are concerned with broader, data-related effects on competition, rather than theories specific to privacy. These data-related theories of exclusion include:

    - The foreclosure of rivals from competitively important data, or means of data collection, through the use of exclusivity agreements, or bundling or

[5] Int'l Competition Network, Report on the Results of the ICN Survey on Dominance/Substantial Market Power in Digital Markets (July 2020), https://www.internationalcompetitionnetwork.org/wp-content/uploads/2020/07/UCWG-Report-on-dominance-in-digital-markets.pdf.

tying of services;

- The use of data to leverage a monopoly from one market to another; and

- Data as an essential facility, to which rivals require access to compete effectively.

- **In a new variation on traditional antitrust theories of competitive foreclosure, several antitrust agencies have expressed concern over "self-preferencing," by digital platforms.** This term of art is used to describe conduct where a dominant platform uses its dual role as the operator of a site where online competition occurs to advantage its own vertically-integrated offerings over third-party products or services offered through the same site. For example, online retailer Amazon has been accused of foreclosing competition from its online marketplace, by prominently feature its own products over those of third-party sellers who rely on the marketplace to compete with those Amazon products.

    - Self-preferencing is not prohibited by most competition laws, which do not impose a general duty of dominant firms to assist their rivals. However, antitrust agencies observe that such conduct may violate abuse of dominance or monopolization prohibitions when it constitutes an established form of exclusionary conduct by a dominant firm, with anticompetitive effects.

    - Agencies also express broader, related policy concerns over the power and control exerted by large digital platforms on privacy and competition in the digital ecosystem.

    - Much of the discussion of self-preferencing does not relate specifically to privacy. However, antitrust authorities in the U.K. have questioned whether platforms have the incentive and power to engage in what might be termed "privacy" self-preferencing, by over-interpreting the data privacy obligations imposed on other market participants while allowing the platforms' own vertically-integrated products or services to comply with more lax privacy requirements.

- **Both antitrust and data privacy agencies are watching closely as Google implements plans to block third-party cookies from its Chrome internet browser.** Privacy authorities are scrutinizing the change, and the alternative technology that Google will implement, for their potential impacts on data privacy. U.S. state attorneys general have brought a joint complaint that alleges, among other claims, that Google's policy change is

an unlawful exercise of monopoly power that excludes competing publishers and advertisers. U.K. antitrust authorities are investigating similar theories.

    - The attention from both regimes raises new questions about whether and when practices that may improve privacy could also violate antitrust law, and, if so, how to address this conflict between the two legal realms.

- **The German competition authority is pursuing an exploitative abuse case that combines antitrust and data privacy law in a unique way.** The German competition agency alleges that Facebook used its market power in social networking services to impose terms of service on users that compelled "excessive" disclosure of personal data—meaning disclosure beyond that which would have been granted in the absence of market power. The case argues Facebook violated privacy law by failing to obtain adequate consent for the collection and combination of Facebook user data i) across the Facebook corporate family of social media services, and ii) with information gathered from third-party websites. The case is unique because it fuses the two areas of law, casting a violation of privacy law as the anticompetitive act in antitrust law. The case is ongoing, and has been referred to the European Court of Justice.

    - Other jurisdictions have not followed suit with similar cases, but many have followed the developments in this German litigation with interest. The case has echoed in broader policy concerns over the power imbalance between certain digital firms and consumers. In particular, there is attention from both antitrust and data privacy agencies to dominant firms that impose "take it or leave it" terms of service, which require individuals to consent to data processing as a condition of using the service.

- **Though rare and early-stage, antitrust cases and policy discussions have also begun to consider whether a dominant firm's efforts to protect consumer data privacy could justify the firm's otherwise anticompetitive conduct.**

    - This is one of the most nascent interactions on the horizon between the two areas of law. Antitrust law has not yet determined whether data privacy protection could constitute a procompetitive justification for conduct that would otherwise violate prohibitions on abuse of dominance.

    - However, the Canadian Competition Tribunal considered this question to some extent in *Commissioner of Competition v. Toronto Real Estate Board*, a 2016

abuse of dominance case against a dominant real estate board.

- The board was accused by the Canadian competition authority of unlawfully excluding online realtors from certain home listing data. In response, the board argued that its exclusionary policies were implemented for the purpose of protecting the data privacy of individuals who listed their homes for sale.

- The Tribunal found that the asserted privacy concerns were pretextual, raised as an afterthought in the face of litigation, rather than a primary reason for the board's exclusionary conduct. Despite this conclusion on the facts, the Tribunal recognized in *obiter dicta* that privacy considerations might justify otherwise anticompetitive practices in competition law, if the evidence indicates that privacy protection was the dominant firm's primary motivation for the misconduct.

  - The research for this Report did not find other antitrust agency cases that consider whether data privacy constitutes a justification for anticompetitive conduct. However, similar arguments—that privacy protection justifies allegedly anticompetitive conduct—have been raised by large digital platforms in defense of private U.S. litigation, in response to complaints lodged with EU competition antitrust authorities, and in response to U.S. Congressional inquiries regarding antitrust law.

  - Agencies have also raised related, but broader, policy concerns over whether digital platforms may be over-interpreting privacy obligations as a means to exclude competitors, and entrench their market power.

- **Collaboration between antitrust and data privacy authorities would be valuable in assessing claims of data privacy as a business justification.** The expertise of privacy authorities could help to inform the factual analysis of whether privacy interests are truly at stake in particular case, and to aid in ensuring an accurate understanding of the scope of protected privacy interests.

- **Data privacy will likely grow in its relevance to abuse of dominance investigations and cases.** Privacy is becoming a more significant factor in consumer decision making within some markets. Antitrust enforcement is continuing to focus on digital markets where data-driven business models are prevalent. Many of these business models rely on the processing of personal data, which creates the potential for privacy issues to arise

within abuse of dominance cases.

D. Cartels and Data Privacy

- **Antitrust Law:** Cartel laws around the world prevent certain agreements between competitors to fix prices, allocate markets or restrict output.

- **To date, there has been little to no antitrust or data privacy agency discussion about interactions between cartels and data privacy.**

    - For antitrust agencies, the primary interest regarding cartels and the digital economy is the potential for algorithms to facilitate unlawful collusion between competitors. This topic has been addressed in antitrust policy reports in multiple jurisdictions. It relates to the broader, shared policy interest with privacy law in promoting transparency and trust in digital markets, which is addressed earlier in the Report.

- Since cartel analysis is often price-related, the analytical challenges raised by a cartel that impacts privacy quality are likely to be similar to those discussed above for measuring and quantifying privacy-related effects on competition.

E. Antitrust Remedies and Data Privacy

- **Antitrust Law:** Once an antitrust law violation is found, courts and antitrust enforcers will impose remedies (or negotiate settlement agreements) that are intended to restore or maintain competition. Those remedies may implicate data privacy in a manner that is distinct from the antitrust law violation itself.

- **Discussion of antitrust remedies is commonly bifurcated into "behavioral" and "structural" remedies**, though both may be imposed in the same matter. A structural remedy involves divestiture or dissolution of a business into separate entities. A behavioral remedy seeks to control the conduct of a business, by preventing or requiring certain action (or both).

- **Overall, the understanding of how data privacy may relate to antitrust remedies is at a very early stage.**

- **Compelled data-access or interoperability remedies have the greatest potential to implicate data privacy, particularly where personal data is involved.** Antitrust behavioral remedies may compel dominant or merging firms to provide rivals with access to data, or ensure interoperability, as a means of restoring or maintaining competition.

    - The topic of such data access or interoperability remedies has taken on new prominence in digital policy discussions, where related theories of harm often focus on the competitive value of data, and the effects of foreclosing rivals from data access.

    - The potential impacts on data privacy from structural remedies, if any, are largely unexplored in agency materials.

- **Antitrust law uses such compelled data access or interoperability remedies sparingly and with restraint.** There are no general obligations in antitrust law to disclose or share competitively important data, even for dominant firms. The concern is that, if used too widely, compelled data access could undermine the incentives of data-driven firms to provide innovative products and services that benefit consumers.

- **Though relatively rare, a small number of litigated and settled antitrust agency cases have considered data privacy in the design of the remedies that were imposed.** There are three different ways in which these antitrust remedies relate to data privacy:

    - Remedies in a U.S. cartel case and a French abuse of dominance case compelled firms to disclose certain personal data held about individuals, in order to restore competition. These remedies were designed to include an opt-out mechanism, through which individuals (whose data would otherwise be subject to remedial disclosure) could elect not to have their personal data disclosed as part of the remedy, or in one case, to withhold certain types of data.

    - Antitrust remedies in mergers and joint ventures have reinforced existing obligations to comply with data privacy law. For example, the European competition authorities required that Google provide EU users with a meaningful choice to grant or deny the use of their health and wellness data, as a condition of the company's acquisition of Fitbit. Similar obligations to comply with data privacy law were recommended by the Colombian competition authority in its review of a joint venture between the three largest Colombian banks.

- Finally, antitrust authorities have imposed merger remedies that require the merging parties to continue to hold data separately. The European remedies in *Google/Fitbit* also included this type of "data silo" obligation, requiring that Fitbit user health and fitness data be stored separately from the data that Google uses for online advertising. While the antitrust goal of such obligations is to limit the likely anticompetitive effects of data combination, there may also be incidental privacy benefits where this type of remedy prevents personal data from being combined and processed across the merging businesses.

- **Ultimately, discussion about data access remedies must be case-specific,** taking into account the types and uses of data by the parties involved, and the specific antitrust market under consideration.

- **This remedies-stage interaction presents a new opportunity for productive collaboration between antitrust and data privacy authorities.** The expertise of data privacy authorities could provide valuable insight for antitrust authorities seeking to understand whether and when data privacy rights or interests are likely to be impacted by antitrust remedies. The remedies employed by data privacy enforcers may inform the design of innovative data-related remedies in antitrust law. The OECD has specifically called for cooperation in the design of remedies.

- **The relevance of data privacy to antitrust remedies, and the complexity of this interaction, is likely to increase** as antitrust enforcement continues to focus on the digital economy.

    - As data privacy law moves toward increasingly robust conceptions of consent—such as preferring opt-in rather than the opt-out models, and greater optionality in consent terms—antitrust authorities may be harder-pressed to craft effective and administrable remedies that center around the consent of individuals.

    - The restoration of competition in some markets may require antitrust remedies that compel ongoing interoperability or data flow, rather than the one-off or episodic data transfers that characterize past antitrust remedies. Antitrust remedies that require ongoing data access may raise more difficult questions around how to account for data privacy.

Conclusion

The time is ripe to develop both theory and practice at the intersection of antitrust and data privacy law. As this Report attests, there is a complex tapestry of interactions emerging between these areas of law. New touchpoints are rapidly appearing as antitrust and data privacy laws both focus on the digital economy. This confluence of attention promises an era of unprecedented interaction between antitrust and data privacy law.

Yet this Report also reveals that theories in this space are often new, and the practice is often unclear. Despite positive progress, most antitrust and data privacy agencies are just beginning to cooperate across their spheres of responsibility. This *status quo* creates the risk of unnecessary or unintended gaps, overlap, tension and even conflict between the two enforcement realms. In the rapidly evolving, high-stakes digital world, such regulatory inefficiencies impose costs and undermine the consumer welfare goals of both antitrust and data privacy law.

The challenge of digital regulation demands cross-agency collaboration. Discourse across the realms of antitrust and data privacy is crucial to build deep agency expertise, concrete, evidence-based theories and cohesive enforcement strategies. Effective collaboration between antitrust and data privacy enforcers promises to bring lasting benefits to consumers, businesses and the agencies themselves. To that end, the Report concludes by identifying several discussion questions where future cross-doctrinal dialogue and collaboration would be particularly valuable.

Future Cross-Agency Discussion Topics on the Antitrust/Data Privacy Intersection

1. **Competition and Privacy Tradeoffs:** Are there tradeoffs between the promotion of competition and the protection of data privacy in law, enforcement or policy? If so, when and to what extent are such tradeoffs likely to occur? How might agencies in each realm assess and understand those tradeoffs?

2. **Privacy Quality and Competition:** When is the quality of privacy protection within a market likely to be affected by competition? How is such privacy quality likely to be affected? Conversely, when might data privacy protection affect competition?

3. **Measuring Competitive Effects on Privacy**: In practical terms, how might antitrust authorities measure the relevant effects of competition on the quality of privacy offered in a given market?

4. **Abuse of Dominance**: What is the relationship between monopolization, competition and privacy? How might monopoly power, or conversely, competition, affect the privacy

protections offered to consumers? What evidence exists to substantiate and understand the views on this relationship?

5. **Business Justifications**: When, if ever, does the protection of data privacy justify otherwise anticompetitive conduct? How might antitrust authorities properly evaluate arguments that a merger or misconduct was engaged in to protect the data privacy of individuals?

6. **Mergers**: How is privacy quality, as it relates to competition, likely to be impacted by mergers or other transactions? What are the accepted theories regarding the effects of mergers, and other corporate transactions, on privacy-related competition?

7. **Remedies***:* How is data privacy relevant to various types of antitrust remedies? How might antitrust remedies be designed to limit unnecessary or unintentional effects on data privacy, particularly where remedies mandate the disclosure of personal data, or impose interoperability obligations on companies that hold personal data?

8. **Assessment and Development of Theories and Practice:** As existing theories on antitrust and data privacy are tested and developed in enforcement and litigation, are those theories proving well-founded, evidence-based and sufficiently broad to explain the various interactions between the two areas of law? Recognizing that this is a nascent intersection of law, how might developments in data privacy or antitrust law (or policy) affect the interactions between these two realms?

Methodology and Scope for the Academic Review

The purpose of this Report is to identify, describe and categorize the perspectives of antitrust and data privacy agencies on the interaction between their regimes. The Report enumerates the wide array of interactions between antitrust and data privacy law to identify their typology and variation. It will be complemented by other reporting on the same topic that is currently being carried out by the GPA Digital Citizen and Consumer Working Group. That work includes deep-dive interviews of antitrust agencies on the practical application of data privacy in their work, and associated views on complements and tensions between regulatory regimes.

The Report is based on a review of publicly available, English-language materials from antitrust and data privacy agencies, with a focus on the jurisdictions that comprise the Global Privacy Assembly Digital Citizen and Consumer Working Group. The research included the review of

more than 200 different agency-related materials, such as enabling legislation, decisions, litigation filings, guidance, speeches, comment submissions and market/sector studies. The review thus reflects the positions agencies have publicly declared on these emerging issues. The Report discussion emphasizes EU, U.K., U.S., Canadian and Australian examples because those jurisdiction have a variety of accessible materials that address this intersection of law.

The research also covered relevant documentation from other entities such as the OECD, the United Nations Conference on Trade and Development (UNCTAD) and the Global Privacy Assembly itself. The research did not expressly include a literature review, but does refer to certain literature where required.[6] Similarly, litigation brought by private parties, rather than agencies, was not the focus of the research but is referenced at times.

The research primarily emphasizes the last 5-7 year period, through to an end date of approximately March 2021 (but at times draws on older or more recent material of particular significance). This recency is not due to an express limitation on the period for the research, but rather a reflection the recent rise in interactions between antitrust and data privacy law. In fact, several significant developments occurred at this intersection of law during the writing of the Report.

This Report is not intended to provide specific recommendations on, or to evaluate the propriety of agency views. However, the Report is intended to be useful in informing such views, by virtue of its identification of areas of convergence or divergence across jurisdictions, as well as opportunities for further development of theory and practice. Though the selection and emphasis of material necessarily reflects judgment, the positions described do not necessarily reflect the views of the author (nor could they all be, given the variation between the perspectives described).

The scope of this Report excludes discussion of the interaction between consumer protection law and privacy law. Though important, and often related to the topics addressed here, those interactions between consumer protection and competition law have already been addressed by the GPA Digital Citizen and Consumer Working Group in a separate, comprehensive report.[7]

[6] For a review of the scholarly literature related to many of the topics covered here, *see* Org. for Econ. Co-operation and Dev. (OECD), Directorate for Financial & Enterprise Affairs Competition Comm., Consumer Data Rights and Competition (Apr. 29, 2020), https://one.oecd.org/document/DAF/COMP(2020)1/en/pdf [*hereinafter* OECD, Consumer Data Rights and Competition – Background Note].

[7] GPA 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, 41st International Conference of Data Protection and Privacy Commissioners (2019), http://globalprivacyassembly.org/wp-content/uploads/2019/11/DCCWG-Report-Albania-2011014.pdf.

The exclusion of consumer protection issues from this Report can, at times, be a somewhat artificial construct. In jurisdictions such as the U.S., data privacy law is a sub-type of consumer protection law. In others, though the legislative roots of consumer protection law and competition law are separate, the same regulatory authority enforces both areas of law. The result is that, at times, agency discussions may blend considerations of competition and consumer protection interests. Particularly in policy discussions, issues may implicate both areas of law and the distinction as to which is being discussed is not always clear. Nonetheless, the Report endeavors to focus specifically on data privacy and competition, leaving aside the considerations, cases and policy of (broader) consumer protection law discussed in the separate GPA report on the intersection of data privacy and consumer protection law.

Though this Report was not limited to the digital economy, interactions between antitrust and data privacy are the most stark, and the most common, in the context of digital policy, law and enforcement. The Report therefore emphasizes the digital economy throughout the discussion. The Report seeks to balance between useful generalizations and country-level specificity. However, it is imperative to note that, as highlighted at various points throughout the discussion, both privacy and antitrust law vary around the world. The interactions between these areas of law will therefore vary as well.

The Report is organized primarily by antitrust topic, for two reasons. First, the Report was written mainly for a privacy audience seeking to understand the landscape of potential interactions with antitrust law. Second, this intersection has tended to draw somewhat more attention from the antitrust side than from the privacy side. This difference may simply reflect the more general economic mandates of antitrust agencies, which are sufficiently broad to encompass topics of privacy-related competition.

Finally, despite differences in the use and meanings around the world, for the purposes of the international discussion in this Report, the terms “antitrust” and “competition” are used interchangeably, as are “data privacy” and “data protection.” Finally, the term “consumer” is used throughout the report to refer to actors who, at times, might be more precisely termed “individuals” (or “data subjects”) in the privacy context, where impingement of privacy is not contingent on a commercial relationship. These terminology differences reflect the distinct mandates of antitrust agencies and data privacy agencies.

Growing Cross-Agency Collaboration in Antitrust and Data Privacy Enforcement

This section considers the current status of inter-agency co-operation between antitrust and data privacy agencies. Though this is a deeply important and related topic to the substance of this Report, the coverage here is kept succinct because the GPA Digital Citizen and Consumer Working Group has already undertaken an in-depth mapping of such co-operation in its other work.[8]

There is no single model of agency responsibility for antitrust law or data privacy law enforcement around the world. In some jurisdictions, antitrust and data privacy law are enforced by separate regulatory authorities. In others, the same regulatory agency has jurisdiction over both antitrust and data privacy law, and sometimes over consumer protection law as well.[9] The specific approaches to collaboration vary by jurisdiction, in a reflection of these structural differences.

Given these differences, the term "antitrust agency" is used in this Report for ease of reference, to mean the executive branch agency with the authority to enforce competition or antitrust law, and acting in that capacity. The term "data privacy agency" is used equivalently, to refer to the agency acting in its legislative or *de facto* authority to enforce data privacy law, such as it is, in each jurisdiction. In countries where both "agencies" are one and the same, the terms are still used to refer to action under each distinct area of authority, which tend to be separate in law.

Just a few years ago, both competition and privacy agencies remarked on the separation between their realms of authority.[10] The European Data Protection Supervisor (EDPS) observed with

[8] GPA, Digital Citizen and Consumer Working Group Annual Report (Oct. 2020) at Annex 2, https://globalprivacyassembly.org/wp-content/uploads/2020/10/Day-1-1_2g-Day-3-3_2h-Version-1_0-Digital-Citizen-and-Consumer-Working-Group-Report-Final.pdf.

[9] OECD, Directorate for Fin. & Enter. Affairs Competition Comm., Quality Considerations in Digital Zero-Price Markets – Background Note by the Secretariat, at 31 (Nov. 28, 2018) [*hereinafter* OECD, Zero-Price Markets – Background Note], https://one.oecd.org/document/DAF/COMP(2018)14/en/pdf (observing that over 30 competition authorities also enforce consumer protection laws). For example, the mission of the Colombian Superintendencia de Industria y Comercio includes the enforcement of data privacy, competition and consumer protection law (among other areas of law), while the U.S. Federal Trade Commission has the authority to enforce both federal data privacy law and antitrust law (in conjunction with the U.S. Department of Justice, Antitrust Division).

[10] Preliminary Opinion of the EDPS, Privacy and Competitiveness in the Age of Big Data: the Interplay between Data Protection, Competition Law and Consumer Protection in the Digital Economy (Mar. 2014),

concern "a tendency, despite obvious synergies like transparency, accountability, choice and general welfare, for EU rules on data protection, consumer protection and antitrust enforcement and merger control to be applied in silos." [11]

As this separation was increasingly acknowledged, it launched a growing dialogue on regulatory cooperation, including efforts like this Report and other GPA projects. Only five years later, the former head of EDPS, Giovanni Buttarelli, issued this rousing call to action: [12]

> We can no longer afford to observe the bureaucratic niceties and jurisprudential silos of competition, consumer and data protection law. From now on, all of these arms of the supervision of the digital economy and society need to be working together and coherently.

Antitrust and data privacy agencies have begun to heed this call to action, with an increasing array of cross-agency collaboration. Recent inter-agency cooperation includes consultations on individual matters,[13] the issuance of joint guidance,[14] new agency collaboration agreements[15] and

https://edps.europa.eu/sites/edp/files/publication/14-03-26_competitition_law_big_data_en.pdf (recommending integration of the data protection rights and the enforcement of competition law); German Monopolies Comm'n (Monopolkommission), Competition Policy: The Challenge of Digital Markets, Special Report No. 68 (Jun. 2015) (same).

[11] EDPS, EDPS Opinion on Coherent Enforcement of Fundamental Right in the Age of Big Data (Opinion 8/2016) 1, 3 (Sep. 2016) (referencing observations in a 2014 EDPS report).

[12] Giovanni Buttarelli, EDPS, Opening Speech at the Youth and Leaders' Summit (Jan. 21, 2019).

[13] *See, e.g.*, Eur. Comm'n Press Release IP/20/2584, *Mergers: Commission Clears Acquisition of Fitbit by Google, Subject to Conditions* (Dec. 17, 2020), https://ec.europa.eu/commission/presscorner/detail/en/ip_20_2484 See e.g. (a recent example of inter-agency cooperation between the EU competition and data protection authorities in the merger investigation).

[14] *See, e.g.*, Competition Comm'n of Singapore, Intellectual Prop. Office of Singapore & Personal Data Protection Comm'n, *Data: Engine for Growth – Implications for Competition Law*, *Personal Data Protection, and Intellectual Prop. Rights* (Aug. 2017) [*hereinafter* Singapore, Data: Engine for Growth]; U.K. Info. Comm'r Off. & CMA, *Competition and Data Protection in Digital Markets: A Joint Statement Between the CMA and the ICO* (May 19, 2021); Autorità Garante della Concorrenza e del Mercato, Autorità per le Garanzie nelle Comunicazioni & Garante per la Protezione dei Dati Personali, *Big Data: Joint Knowledge Survey Guidelines and Policy Recommendations* (Indagine Conoscitiva Congiunta Linee Guida e Raccomandazioni di Policy) (July 2019) (It.), https://www.agcm.it/dotcmsdoc/allegati-news/Big_Data_Lineeguida_Raccomandazioni_di_policy.pdf (joint survey and recommendations of the Italian competition, data protection and communication authorities); Press Release, Italian Competition Authority, *Big Data AgCom, AgCM and Data Protection Authority Survey Published* (Feb. 10, 2020) (joint sector inquiry on big data).

[15] *See, e.g.*, U.K. CMA & ICO, Memorandum of Understanding Between the Information Commissioner and the Competition and Markets Authority (establishing a framework for cross-agency cooperation and information sharing); Netherlands Authority for Consumers and Markets & Authority for Personal Data (Autoriteit Consument en Markt en Autoriteit Persoonsgegevens), Collaboration Protocol Between the Netherlands Authority for Consumers and Markets and Data Protection Authority, ACM (Samenwerkingsprotocol tussen Autoriteit Consument en Markt en Autoriteit Persoonsgegevens, ACM), Staatscourant (Nov. 3, 2016)

more. From a macro-level perspective, antitrust and data privacy cooperation is increasingly recognized by agencies as a matter of strategic importance.[16] There have been notable structural efforts to facilitate collaboration on investigations and best practices in jurisdictions such as the EU,[17] U.K.[18] and Singapore.[19] These new efforts at regulatory cooperation are mapped in-depth in a separate report by the GPA Digital Citizen and Consumer Working Group, and thus not reiterated in detail here.[20]

Despite these positive developments, inter-agency collaboration is far from well-established in matters that implicate data privacy and competition. Cooperation across these two legal realms remains both an important challenge and a shared opportunity. Without a cohesive approach to regulation, agencies risk problematic gaps, assumptions or overlaps, and harm from inconsistent

https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/convenant_acm-ap.pdf. This collaboration agreement between the Dutch privacy authority and Dutch consumer protection and competition authority is described in English in the Global Privacy Assembly, Digital Citizen and Consumer Working Group Annual Report, *supra* note 8, Appendix G at 23.

[16] *See, e.g.*, Maarten Stassen, Frederik Van Remoortel, & Heidi Waem, *Belgium – National GDPR Implementation Overview*, § 1.2 Guidelines (Sep. 2020), https://www.dataguidance.com/notes/belgium-national-gdpr-implementation-overview#:~:text=2.1.-,Main%20regulator%20for%20data%20protection,Commission%2C%20on%2025%20May%202018 (identifying improved data protection through collaboration with other agencies as a strategic objective); Giovanni Buttarelli, EDPS, Opening Statement for Panel on Digital Rights and Enforcement at the 10th Computers, Privacy and Data Protection Conference at 4 (Jan. 26, 2017) (describing regulatory cooperation among competition, privacy and consumer protection authorities as "a strategic, long term issue").

[17] The European Digital Clearinghouse, established in 2017, is a platform to facilitate cooperation, dialogue and information sharing between competition, consumer protection and privacy regulators. European Data Protection Supervisor, *Big Data & Digital Clearinghouse*, https://edps.europa.eu/data-protection/our-work/subjects/big-data-digital-clearinghouse_en (last visited May 12, 2021).

[18] CMA, Policy Paper: Digital Regulation Cooperation Forum Launch Document (July 1, 2021), https://www.gov.uk/government/publications/digital-regulation-cooperation-forum (announcing the formation of a Digital Regulation Cooperation Forum between the U.K. competition agency, privacy agency and Office of Communications to "support regulatory coordination in digital markets, and cooperation on areas of mutual importance.").

[19] Competition & Consumer Comm'n of Singapore, Community of Practice for Competition and Economic Regulations, https://www.cccs.gov.sg/approach-cccs/for-government-agencies/community-of-practice#:~:text=Established%20in%20December%202013%2C%20the,competition%2C%20consumer%20protection%20and%20regulatory (last updated Oct. 19, 2020) (describing the Singaporean Community of Practice for Competition and Economic Regulations,"an inter-agency platform for government agencies to learn about latest local and overseas market developments and share best practices and experiences on competition, consumer protection and regulatory issues.").

[20] Global Privacy Assembly, Digital Citizen and Consumer Working Group Annual Report, *supra* note 8, at Annex 2: Digital Citizen and Consumer Working Group Mapping of Regulatory Intersections and Actual Collaborative Actions Table.

or even conflicting positions in policy or law.[21] Enforcement by one realm could advance its own objectives while unnecessarily, or even unwittingly, eroding those of the other.

Particularly in the digital economy, competition and data privacy authorities can no longer achieve their goals in isolation.[22] Coordination between these agencies, and consumer protection authorities, will play an important role in fostering consumer welfare and trust in the digital economy, stimulating demand for privacy-enhancing services, and advancing agency mandates.[23]

Part I: Understanding Complementarity and Tension at the Roots of Antitrust and Data Privacy

This Part considers the legal roots of the interactions between antitrust and data privacy law. It begins with discussion of the definitional ambiguity in the terms "privacy" and "privacy law." The Report then adopts a working definition of "privacy law," as it is understood to intersect with antitrust law. Then, this Part considers the objectives commonly expressed in competition legislation and privacy legislation around the world, and how the objectives of each realm may interact. The final section in this Part identifies and summarizes three shared interests emphasized in both antitrust and data privacy policy: i) the promotion of consumer trust in digital markets, ii) the encouragement of data portability, and iii) the promotion of consumer choice (and concern over distortion of such choice, particularly in digital markets).

1. Framing Privacy Law Concepts: Rights, Interests and Reconcilability with Antitrust Law

Throughout its legal history, the definition of privacy has been a divisive and slippery concept. From Samuel Warren and Louis Brandeis's influential conception of privacy as "the right to be

[21] William P. Barr, Att'y Gen., U.S. Dep't of Justice, Remarks at the National Association of Attorneys General 2019 Capital Forum (Dec. 10, 2019) (observing that "[h]igh level coordination in our review of market-leading online platforms also helps avoid imposing conflicting obligations or inconsistent policy positions. This requires coordination both within and outside DOJ.")

[22] OECD, Directorate for Fin. & Enter. Affairs Competition Comm., Executive Summary of the Discussion on Quality Considerations in the Zero-Price Economy - Annex to the Summary Record of the 130th Meeting of the Competition Committee held on 27-28 November 2018, at 5 (2018) [*hereinafter* OECD, Zero-Price Economy – Annex], https://one.oecd.org/document/DAF/COMP/M(2018)2/ANN9/FINAL/en/pdf (noting for zero-price markets that "a key challenge is to improve cooperation and information sharing between competition, privacy and data protection and consumer protection regulators").

[23] *See, e.g.*, Preliminary Opinion of the EDPS, Privacy and Competitiveness in the Age of Big Data: The Interplay between Data Protection, Competition Law and Consumer Protection in the Digital Economy (Mar. 26, 2014) (closer collaboration across policy spheres could strengthen competition and stimulate the market for privacy-enhancing services).

let alone,"[24] to our modern collection of privacy rights and interests, there has been little broadly accepted meaning of "privacy." Scholars acknowledge this definitional ambiguity, describing the concept of privacy as "chameleon-like," "vague and evanescent," "protean," "in disarray" and suffering from "an embarrassment of meanings."[25]

The term "privacy law" can be similarly nebulous. It evokes a wide array of meanings both within and across jurisdictions. "Privacy law" can refer to constitutional, consumer protection or tort law, sectoral or omnibus legislation, spatial, decision or information privacy protection, privacy from governmental or non-governmental intrusion and more.

Without diminishing the importance of this debate over the meaning of "privacy" and "privacy law," this Report does not seek to answer how each facet of privacy (or privacy law) might potentially relate to competition. Instead, the Report frames its discussion by accepting the practical reality of agency views—from both the antitrust and data privacy realms—on the specific conceptions of privacy that are relevant to competition.

This approach narrows the scope of the privacy law discussed in this Report, in several respects. First, it means considering the privacy obligations of only of non-governmental entities. There are often distinct privacy laws or legislative provisions that apply to governmental use of information, but antitrust law is primarily concerned with the role of data in enterprise and competition—not the use of data by government.

Second, it results in a focus on informational or *data* privacy, and in particular, an individual's legally protected right or interest to control the processing of their personal information. Despite the many threads of what privacy means, when it comes to data privacy, "[t]he weight of the consensus about the centrality of privacy-control is staggering."[26] The focus of data privacy law around the world has tended to be on consent-based models that enable consumers to control the collection and processing of their data. This conception of data privacy is also the most relevant to the operation of modern commerce and competition, which has come to depend in a myriad of ways on the collection, use and sale of data, both personal and otherwise.

[24] Samuel D. Warren and Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 195 (1890).

[25] Daniel J. Solove, *A Taxonomy of Privacy*, 154 U. PA. L. REV. 477, 479-80 (2006) (noting these many observations of the difficulty in defining privacy); Joshua A.T. Fairfield & Christoph Engel, *Privacy as a Public Good*, 65 DUKE L.J. 385, 406 (2015) ("[p]rivacy theorists differ famously and widely on the proper conception of privacy").

[26] Paul M. Schwartz, *Internet Privacy and the State*, 32 CONN. L. REV. 815, 820 (2000).

Today, approximately 130 jurisdictions around the globe have some form of data privacy or data protection legislation, with even more countries poised to pass their first privacy laws.[27] Those laws include a wide variety of rights and interests that give further shape to how antitrust authorities understand the concept of data privacy. Data privacy law exists as a growing collection of rights and interests related to personal data access, portability, correction, deletion, transparency of processing and minimizing data collection. Some laws include the rights around automated decision making, the right to be forgotten, anti-discrimination and beyond—or frame data privacy itself as a fundamental right. These many facets of modern data protection law contribute meaning to data privacy, and shape its interaction with antitrust law and competition policy.

This working definition of non-governmental data privacy rights and interests gives some shape to how privacy is conceived at its intersection with antitrust law and policy. But, even within this definition, there are deep differences in the doctrinal roots of privacy law that may influence its reconciliation with antitrust. In some jurisdictions, like the European Union and its member states, data protection is conceived of as constitutionally protected right,[28] inalienable and foundational to conceptions of freedom and human dignity.[29] The powerful new GDPR is designed to protect the rights of individual data subjects to control their personal data, and it endows those individuals with a formidable array of rights.[30] The deep legal roots of data protection law are evident in the starting legal premise of GDPR, which prohibits the processing of personal data, except where certain lawful grounds for such processing are established.[31]

---

[27] United Nations Conference on Trade and Dev. (UNCTAD), *Data Protection and Privacy Legislation Worldwide* (Feb. 4, 2020), https://unctad.org/page/data-protection-and-privacy-legislation-worldwide (noting 128 of 194 countries surveyed had some form of data privacy or protection legislation).

[28] Charter of Fundamental Rights of the European Union, Art. 8(1), 2012 O.J. (C. 326) 391, 397 (describing a fundamental right to "the protection of personal data"); Consolidated Version of the Treaty on the Functioning of the European Union, 2012 O.J. (C 326) 47, Art. 16(1) [*hereinafter* TFEU] ("Everyone has the right to the protection of personal data concerning them"). In addition to data protection, privacy is also protected as a distinct human right in European law.

[29] *See, e.g.*, Eur. Data Prot. Supervisor (EDPS), *The EDPS Strategy 2020-2024: Shaping a Safer Digital Future*, at 5 (2020) https://edps.europa.eu/sites/default/files/publication/20-06-30_edps_shaping_safer_digital_future_en.pdf ("We must continue to stake our claim as advocates for the fundamental rights to data protection and privacy, because it is the cornerstone of individual freedom and democracy").

[30] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), Art. 1, 2016 O.J. (L. 119) 1 [*hereinafter* "GDPR"] (protecting the privacy of "natural persons with regard to the processing of personal data and rules relating to the free movement of personal data"). *See, e.g.*, *id.* at Art. 15 (access), Art. 16 (rectification), Art 17 (erasure), Art 20 (portability).

[31] GDPR, *id.* at Art. 6 (processing lawful only based on the listed grounds).

Other jurisdictions, like Australia and Canada, conceive of data privacy law in terms of principles, rather than in terms of rights. Privacy principles are enshrined in omnibus legislation that imposes data protection obligations.[32] However, individuals are not endowed with data privacy "rights," nor are there constitutional roots to data protection.[33]

In still other jurisdictions, like the U.S., federal data privacy is a sub-category of consumer protection law. When it comes to data processing by companies, there is no constitutional or other "right" to data privacy, outside of certain sectoral legislation. There is no omnibus federal data privacy legislation in the U.S. The *de facto* privacy agency, the Federal Trade Commission (FTC), has no express legislative mandate to protect privacy, other than in certain sectoral regulations. Instead, the FTC has constructed data privacy principles gradually, using its power to combat unfair and deceptive acts and practices against consumers.[34] Subject to the limits of consumer protection and state law, personal data is, by and large, free to be processed in the U.S.[35]

Finally, these legal roots of data privacy seem to be in a state of evolution. In the U.S., there is new state-level legislation adopting privacy rights that look more akin to the GDPR than to U.S. federal consumer protection law.[36] Australia has established a new consumer data right, although it is only applicable in certain designated sectors.[37] Meanwhile, the Privacy Commissioner of Canada is advocating for a shift from the narrower data protection framing of Canadian data privacy legislation to a rights-based foundation, and has called for the recognition of privacy as a tenet of freedom, democracy and equality.[38] Despite the lack of right-based legislation, Canadian

[32] *Personal Information Protection and Electronic Documents Act, S.C. 2000*, c.5 (Can.); *The Federal Privacy Act 1988*, No. 119 (Austl.).

[33] As with the remainder of this Report, this discussion of *data* privacy leaves aside other types of privacy that are rights-based within these jurisdictions, such as rights against unreasonable invasions of privacy by the state.

[34] 15 U.S.C. § 45(a).

[35] *See, e.g.*, Giovanni Buttarelli, EDPS, Opening Speech at the Youth and Leaders' Summit (Jan. 21, 2019) (observing the distinction that in the U.S. "in the name of free markets, data is another locus for competition between companies and consumers" whereas in Europe "according to the European Convention on Human Rights and the Charter of Fundamental Rights of the EU, data doesn't belong to anyone but privacy is something inalienable and personal data is something to be treated with respect.").

[36] The California Consumer Privacy Act of 2018, Cal. Civ. Code § 1798.100 (2018); Consumer Data Protection Act, SB 1392 (2021) (amending Code of Virginia, Title 59.1, chapter 52, consisting of sections numbered 59.1-571 through 59.1-581). The California legislation has been compared more closely to GDPR, but both are significant advances in U.S. state privacy law.

[37] Australian Competition and Consumer Comm'n, *Consumer Data Right (CDR)*, https://www.accc.gov.au/focus-areas/consumer-data-right-cdr-0 (explaining that in November 2017, the Australian Government announced a new consumer data right).

[38] Daniel Therrien, Privacy Comm'r of Canada, Remarks at a Federal Access to Information and Privacy Community Meeting: Modernizing Federal Privacy Laws to Better Protect Canadians (Mar. 9, 2020),

courts have recognized the quasi-constitutional status of privacy.[39]

These conceptual differences in the roots of data privacy law (and their evolution) may impact the reconciliation with antitrust law. The presence of weighty, rights-based conceptions of privacy commands from antitrust, strengthening the case for express consideration of privacy in competition analysis.[40] Such analysis presents an "apples to oranges" reconciliation between the fundamental human right of privacy, and the economic interests advanced by competition law. Where there are tradeoffs between competition and privacy, this analysis may raise complex questions for agencies, scholars and courts. How should tradeoffs be analyzed at the edges between a dignitary right of individuals to control their person information, and the collective benefits of data-driven competition? Is there a means of protecting or achieving both?

The analysis will look different in jurisdictions like the U.S., where competition and privacy are both framed in economic regulatory terms. The shared economic roots make for an "apples to apples" comparison between consumer welfare impacts on competition, and consumer protection harms. In the face of any tradeoffs between the two, it leads to questions like, "Will consumers' economic well-being be improved in this market by more data privacy protection, or greater data-driven competition?" Striking the optimal balance between the two interests may not be easy, but there are adjacent roots in economic regulation. This commonality may ease or simplify the reconciliation with antitrust law in those jurisdictions where privacy is conceived of more narrowly, as a consumer protection interest.

These differences in the legal roots of data privacy echo throughout the coverage of this Report. Regulatory agencies within the European Union have paid extensive attention to the reconciliation of competition law and data privacy law, at least in part because it is demanded by the robustness of the GDPR (and similar member state laws), and its corresponding relevance to data-driven competition and antitrust law. Though other jurisdictions have thoughtfully contemplated this interface between antitrust and data privacy, the issue may command a less pressing role in agency dialogue. This reflects, at least in part, the less foundational status of data

https://www.priv.gc.ca/en/opc-news/speeches/2020/sp-d_20200309/; Off. of the Privacy Commissioner of Canada, 2018-2019 Annual Report to Parliament on the *Privacy Act* and the *Personal Information Protection and Electronic Documents Act* 11-12 (2019) (calling for new Canadian data privacy legislation to have "a rights-based foundation").

[39] Alberta (Information and Privacy Commissioner) v. United Food and Commercial Workers, Local 401, [2013] 3 SCR 733 (data protection legislation has a quasi-constitutional status "because of the fundamental role privacy plays in the preservation of a free and democratic society" (citing *Lavigne v. Canada (Office of the Commissioner of Official Languages)*, [2002] 2 S.C.R. 773, at para. 24 among other decisions)).

[40] Peter Swire, Ohio State Univ., Ctr. for Am. Progress, Presentation at the International Association of Privacy Professionals Annual Conference: Privacy and Antitrust (Mar. 2008).

privacy in the laws of those jurisdictions.

2. Why Are Antitrust and Data Privacy Law Beginning to Interact?

Antitrust and data privacy are interacting in new and unprecedented ways. Much of this Report focuses on what those interactions are, and how they might be understood. This section steps back to discuss the broader question of *why* antitrust and data privacy are now interacting.

There appear to be several reasons why antitrust and data privacy law are interacting more than ever before. First, there has been a massive expansion of the digital world, and with it the ubiquity and economic importance of consumer data. From search and social media, to online shopping, banking and health, data-driven services have become deeply ingrained in consumers' everyday lives. In this new digital landscape, privacy enforcers are intensely focused on protecting individuals from unlawful data processing. Meanwhile, antitrust law is focused on the role of data in driving competition, particularly in the digital economy where technology giants have begun to wield power over data-driven markets. These enforcement regimes are meeting in the digital economy, where privacy and personal data have become material to competition.

Second, and relatedly, there has been a dramatic rise in both data privacy law and antitrust enforcement. Though the roots of privacy law are much older, it is only over the last twenty-five years or so that *data* privacy law has grown into a robust and widespread area of legal doctrine. Today, approximately 130 jurisdictions have some form of data privacy or data protection legislation.[41] At least twenty others report that draft data privacy legislation is under consideration.[42] Data privacy law enforcement has become a regular occurrence. This tidal wave of law and enforcement has brought about an intense, global emphasis on data privacy in policy, law and day-to-day business operations.

At the same time, antitrust enforcement has seen its own global revival in recent years. There has been an avalanche of antitrust scrutiny, much of it directed toward large digital platforms and their data-driven competition practices. These digital platforms are the subject of several seminal agency cases, investigations, industry reports and frequent attention from policy and lawmakers, as reflected throughout this Report. These digital businesses are often global in nature, and this

[41] United Nations Conference on Trade and Dev. (UNCTAD), *Data Protection and Privacy Legislation Worldwide* (Feb. 4, 2020), https://unctad.org/page/data-protection-and-privacy-legislation-worldwide (noting 128 of 194 countries surveyed had some form of data privacy or protection legislation).

[42] *Id.* (full data reporting as of February 27, 2021).

has meant antitrust attention from enforcers in many jurisdictions.

Third, antitrust and data privacy law share a common desire to benefit consumers, as well as many granular policy interests. The shared objectives and policy interests of these areas of law are discussed in depth in the following sections of this Report.[43]

These new economic, legal and policy developments are producing more and more interactions between privacy and antitrust. Enforcers in both realms are interested in many of the same business practices and market phenomena. Both are seeking to improve the well-being of consumers (although each has different goals and means of achieving this outcome). More than ever before, consumers are choosing products and services based on privacy features, making privacy and competition important in certain markets. The result is an array of novel interactions between competition and privacy, as described throughout this Report.

These interaction between antitrust and data privacy are also rapidly expanding. A multitude of jurisdictions, such as Brazil, India, China and certain U.S. states, are enacting their first-ever omnibus privacy laws. Longer-established laws are now being expanded through legislative reform in jurisdictions such as Canada, Singapore and Japan, and through the interpretation of laws like the powerful new GDPR. At the same time, the digital economy continues to be a top priority for antitrust enforcers around the globe. This confluence of attention from both realms promises an era of unprecedented interaction between the two areas of law.

[43] See Part I.3. Legislative Objectives and Agency Mandates: Individual Consumer Protection or Overall Economic Efficiency and Part I.4. Shared Policy Interests and Concerns: Trust in Markets, Data Portability and the Impact of Demand-side Distortions in Consumer Choice.

3. Legislative Objectives and Agency Mandates: Individual Consumer Protection or Overall Economic Efficiency

Antitrust and data privacy law are often described as complementary, because the two regimes both seek to benefit consumers.[44] However, each legal realm has its own distinct objectives through which it pursues such consumer benefits: privacy law seeks to protect individual's data privacy rights and interests, while antitrust law works to ensure efficient competition in the marketplace.

Data privacy legislation often contains objectives that emphasize the protection of rights or interests of individuals.[45] A primary goal of data privacy law is to ensure that individuals have effective control over their data, and can choose how it is processed.[46] The legislative objectives, and the design of privacy laws, reflect that privacy rights and freedoms are held by natural persons.

Several jurisdictions also include legislative objectives or provisions about balancing the legitimate interests of organizations to process data,[47] but primacy tends to be place on the protection of individuals' rights or interests throughout the legislation. For example, the trigger for the application of many privacy laws is the personal nature of the data at issue.[48] This is not to suggest that privacy law provides only individualized benefits—the protection of privacy rights accrues collectively to society, including through the important role privacy plays in maintaining freedom and democracy.[49] Rather, it is to point out that the stated legislative objectives focus on the protection of individual rights or interests (even if the pursuit of those objectives results in a collective benefit).

Around the world, one of the most widely articulated objectives of antitrust law is to improve consumer welfare through competition.[50] Antitrust law combats mergers and misconduct that reduce consumer welfare, either by raising prices, lowering quality or reducing output relative to competitive levels. By maintaining competition in markets, antitrust law seeks to achieve lower prices, higher outputs, better quality and more innovation, to the benefit of consumers. This consumer welfare goal is typically expressed in legislation in terms of economic efficiency,[51] though the concepts of welfare and efficiency are not necessarily synonymous. See **Figure 1. Objectives in Competition Legislation and Agency Mandates: A Selection of Jurisdictions with Both Efficiency and Distributional Goals,** below, listing the objectives from the competition legislation of several jurisdictions, many of which include reference to efficiency.

[44] *See, e.g.,* Preliminary Opinion of the EDPS, *supra* note 23; OECD, Consumer Data Rights and Competition – Note by Colombia, at 2 (May 14, 2020) https://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=DAF/COMP/WD(2020)42&docLanguag

e=En (describing data privacy and competition regimes as playing "a complementary role in achieving the wellbeing of consumers and the market itself"); U.K. Info. Comm'r Off. & CMA, Competition and Data Protection in Digital Markets: A Joint Statement Between the CMA and the ICO (May 19, 2021) at 30 (describing the agencies' "shared view that our overlapping objectives regarding competition and data protection in the context of the digital economy are strongly aligned and complementary").

[45] *See, e.g.*, GDPR, *supra* note 30, at Art. 1 (subject-matter and objectives) ("This Regulation protects fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data."); *Personal Data Act 2018*, Chapter I: General Provisions, Art. 1, "Purpose and Objectives" (Nor.), https://lovdata.no/dokument/NL/lov/2018-06-15-38/*#KAPITTEL_2 (implementing objectives from GDPR Art. 1); *Data Protection Act 2018*, Part 1, § 2, "Protection of Personal Data" (U.K.) (the Act "protect[s] individuals with regard to the processing of personal data"); *The Privacy Act 1988,* No. 119, Part I, § 2A "Objects of this Act" (Austl.) (objectives of data privacy law include "to promote the protection of the privacy of individuals"); *Personal Information Protection and Electronic Documents Act, S.C. 2000*, c.5, Part 1, § 3 "Purpose" (Can.) (the purpose of the act is to establish rules that govern information privacy "in a manner that recognizes the right of privacy of individuals").

[46] *See, e.g.*, U.K. Info. Comm'r Off. & CMA, Competition and Data Protection in Digital Markets: A Joint Statement Between the CMA and the ICO (May 19, 2021) at 16 (noting the U.K. data protection framework "seeks to ensure that individuals have effective control over the processing of their personal data and are empowered to make informed and granular choices over that processing.").

[47] *See, e.g.*, *Personal Information Protection and Electronic Documents Act* (PIPEDA), S.C. 2000, c.5, Part 1, § 3 "Purpose" (Can.) (recognizing "the need of organizations to collect, use or disclose personal information for purposes that a reasonable person would consider appropriate in the circumstances."); *The Privacy Act 1988*, No. 119, Part I, § 2A "Objects of this Act" (Austl.) (Objectives of data privacy law include "recogniz[ing] that the protection of the privacy of individuals is balanced with the interests of entities in carrying out their functions or activities. . .").

[48] Paul M. Schwartz & Daniel J. Solove, *Reconciling Personal Information*, 102 CAL. L.R. 877, 879 (noting that the existence of personally identifiable information is "foundational to any privacy regime" because it triggers the applicability of privacy laws). *See, e.g.*, Children's Online Privacy Protection Act, 15 U.S.C. §6502 (2006) (prohibiting certain collection of "personal information" from a child); GDPR, *supra* note 30 at Art. 2 (applicable to personal data).

[49] EDPS, The EDPS Strategy 2020-2021: Shaping a Safer Digital Future, at 5 (2020) https://edps.europa.eu/sites/default/files/publication/20-06-30_edps_shaping_safer_digital_future_en.pdf ("We must continue to stake our claim as advocates for the fundamental rights to data protection and privacy, because it is the cornerstone of individual freedom and democracy."); Peter Hustinx, EDPS, *Data Protection and Competition: Interfaces and Interaction, the Data Protection Law in the Context of Competition Law Investigations* 5 (June 13, 2013) ("…the violation of these rules harms the consumer/individual/data subject, and they also address the wider public interest of a free and open society based on the rule of law and not only on survival of the most powerful.").

[50] The consumer welfare goals of modern antitrust law are classically described in Reiter v. Sonotone Corp., 442 U.S. 330, 343 (1979) ("Congress designed the Sherman Act as a 'consumer welfare prescription'"). Although the consumer welfare standard has long been the subject of debate, it remains the stated goal of antitrust law in many jurisdictions. *See, e.g.*, Christine S. Wilson, Comm'r, FTC, Welfare Standards Underlying Antitrust Enforcement: What You Measure is What You Get, Keynote Address at the George Mason Law Review 22nd Annual Antitrust Symposium: Antitrust at the Crossroads?, at 1 (Feb. 15, 2019), https://www.ftc.gov/system/files/documents/public_statements/1455663/welfare_standard_speech_-_cmr-wilson.pdf (noting that the consumer welfare standard has been "the yardstick used to evaluate mergers and competitive conduct for more than 40 years" in antitrust law); Eur. Comm'n, Guidance on the Commission's Enforcement Priorities in Applying Article 82 [now 102] of the EC Treaty to Abusive Exclusionary Conduct by Dominant Undertakings, 2009 O.J. (L 2009/C 45/02), at ¶ 19, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52009XC0224(01)&from=EN ("The aim of the Commission's enforcement activity…is to ensure that dominant undertakings do not impair effective competition by foreclosing their

Competition law thus seeks to benefit consumers through a broad, economic efficiency prescription, rather than the individualized rights or interests that are characteristic of privacy law. Competition legislation is not framed in terms of the "rights" or "interests" of individuals to the protection of competition (although parties injured by anticompetitive conduct can often pursue private rights of action for their loss in several jurisdictions). Though the promotion of competition, like the protection of privacy, benefits individual consumers, antitrust achieves this benefit collectively, through economic efficiency.

Figure 1. Objectives in Competition Legislation and Agency Mandates: A Selection of Jurisdictions with Both Efficiency and Distributional Goals

- The Canadian Competition Act, "Purpose of Act" includes to "promote the efficiency and adaptability of the Canadian economy" and "ensure that small and medium-sized enterprises have an equitable opportunity to participate in the Canadian economy."[52]

- The Belgian Competition Act is described as having objectives that are "twofold: to guarantee the right of individual firms to do business in the markets of their choice, within clear and plainly circumscribed limits; and to create a framework in which businesses and individuals alike reap the favourable effects of competition on prices and product quality."[53]

- The Danish Competition Act indicates that "[t]he purpose of this Act is to promote efficient resource allocation in society through workable competition for the benefit of undertakings and consumers."[54]

competitors in an anti-competitive way, thus having an adverse impact on consumer welfare…."); *Competition and Consumer Act 2010*, Vol. I, Part I, § 2 (Austl.) (including a legislative objective of "enhance[ing] the welfare of Australians").

[51] Donald F. Turner, *The Durability, Relevance, and Future of American Antitrust Policy*, 75 CAL. L. REV. 797, 798 (1987) ("Antitrust law is a procompetition policy. The economic goal of such a policy is to promote consumer welfare through the efficient use and allocation of resources, the development of new and improved products, and the introduction of new production, distribution, and organizational techniques for putting economic resources to beneficial use . . . .").

[52] R.S.C., 1985, c. C-34, Part I, § 1.1.

[53] OECD, Belgium: Competition Law and Policy in 1997-1998 at 3 (1998), https://www.oecd.org/belgium/1822389.pdf.

[54] *The Danish Competition Act 2018*, Consolidation Act No. 155, Part 1, § 1, https://www.en.kfst.dk/media/50102/engelsk-oversaettelse-af-lovbkg-155-2018.pdf.

- Norwegian Competition Act (translated) indicates that the purpose of the act is to promote competition to contribute to the "efficient use" of society's resources, and that in the application of the legislation, "special consideration shall be given to the interests of consumers."[55] The Norwegian Competition Authority describes its mission as "to help ensure efficient use of the society's resources by promoting competition, for the benefit of consumers and businesses in various national markets."[56]

- The Australian Competition and Consumer Act's legislative objective is to "enhance the welfare of Australians through the promotion of competition and fair trading and provision for consumer protection"[57]

- The Singapore Competition Act provides that the functions of the competition authority include "to maintain and enhance efficient market conduct" and "to promote fair trading practices among suppliers and consumers and enable consumers to make informed purchasing decisions in Singapore"[58]

- The Philippine Competition Act Declaration of Policy includes "constitutional goals for the national economy to attain a more equitable distribution of opportunities" and also to "enhance economic efficiency."[59]

- The German Competition Act provides that (translated to English) "[c]ompetition rules are provisions which regulate the conduct of undertakings in competition for the purpose of counteracting conduct in competition which violates the principles of fair competition or effective competition . . . ."[60]

[55] *Act on Competition Between Enterprises and Control Of Business Combinations* (Competition Act) (Konkurranseloven), 2004, nr. 12, § 1 (Nor.), https://lovdata.no/dokument/NL/lov/2004-03-05-12 - KAPITTEL_1 (English translation).

[56] Konkurransetilsynet (Norwegian Competition Authority), *About Us*, https://konkurransetilsynet.no/norwegian-competition-authority/?lang=en (last visited May 23, 2021).

[57] *Competition and Consumer Act 2010*, Vol. I, Part I, § 2 (Austl.).

[58] *Competition Act 2018*, Ch. 50(B), § 6(1)(a) and (ea), (Sing.).

[59] *The Philippine Competition Act (R.A. 10667) 2015*, Ch. I, § 2.

[60] *Act Against Restraints of Competition 2013*, as last amended by Article 10 of the Act of 12 July 2018 § 24 (2) (Ger.).

- The European Commission Treaty on the Functioning of the European Union (TFEU) Preamble includes acknowledgement that action is required to achieve, among other things "fair competition."[61] Though not exclusive to competition law, economic policy provisions of TFEU specify that Member States and the Union shall act "in accordance with the principle of an open market economy with free competition, favouring an efficient allocation of resources…"[62] and "in accordance with the principle of an open market economy with free competition."[63] The Commission's website similarly reflects that "[c]ompetition policy is about applying rules to make sure companies compete fairly with each other," which "encourages enterprise and efficiency."[64]

  Note: The complete objectives, as stated in the above legislation, are not included here for every jurisdiction, due to length.

Unsurprisingly, the missions or mandates of the agencies who enforce competition[65] and privacy law[66] tend to reflect the respective legislative objectives of economic efficiency or individual privacy protection. These agencies are generally tasked with the pursuit of the legislative objectives. In some instances, the mandates or missions of competition agencies are expressed separately from the objectives but still within the legislation, and in other instances, the missions are stated only on the agency's website.

[61] TFEU, supra note 28, at Preamble.

[62] *Id.* at Art. 120.

[63] *Id.* at Art 119.

[64] Eur. Comm'n, *Competition: Making Markets Work Better*, 3–4 (2013) https://op.europa.eu/s/paxc.

[65] *See, e.g.*, Norwegian Competition Authority (Konkurransetilsynet), Norwegian Competition Authority – About Us, https://konkurransetilsynet.no/norwegian-competition-authority/?lang=en (last visited May 10, 2021) (the agency mission includes "to help ensure efficient use of the society's resources by promoting competition, for the benefit of consumers and businesses…").

[66] *See, e.g.*, EDPS, *About*, https://edps.europa.eu/about-edps_en ("Our general mission is to monitor and ensure the protection of personal data and privacy when EU institutions and bodies process the personal information of individuals…) (last visited May 13, 2021).

These distinct objectives and mandates echo throughout each agency's framing of shared policy issues. For example, both privacy[67] and antitrust agencies[68] have examined the role of "big data" in the economy in recently policy reports. But while data privacy enforcers are concerned with the implications and effects of big data on the privacy of individuals, competition law is interested in the economic value and commercial implications of big data. Privacy enforcers observe that "Big Data . . . does not always involve personal data,"[69] and draw distinctions between data that is personal or non-personal. Competition authorities are less concerned with this difference, focusing instead on the economic effects related to data, regardless of whether it is identified or identifiable to individuals.[70] The different objectives of each regime are also reflected in the breadth of the policy framing—antitrust agencies tend to investigate policy issues on somewhat broader terms, such as several recent "digital policy" or "digital platforms" reports.[71] This broader framing often makes sense in light of antitrust authorities' more general, economic efficiency goals.

a. Competition Law Objectives Beyond Economic Efficiency: Fairness and Opportunities for Businesses

In addition to economic efficiency, several jurisdictions include distributional goals in their competition legislation, such as fairness or the provision of equitable opportunities for businesses. See **Figure 1. Objectives in Competition Legislation and Agency Mandates: A**

[67] Giovanni Buttarelli, EDPS, FutureTech Congress– Keynote Speech for the Panel: The Impact of the GDPR on Solutions Based on Big Data Processing, at 2 (May 25, 2017) (observing that "Big Data analytics are often a threat to privacy and data protection. . . . Data constitute one of the biggest challenge for data protection regulators."); Big Data: Joint Knowledge Survey Guidelines and Policy Recommendations (July 2019) (It.), *supra* note 14; U.K. Info. Comm'rs Office (ICO), Big Data Artificial Intelligence, Machine Learning and Data Protection (2017); ICO, Big Data and Data Protection Guide (July 2014); Datasylnet (Norwegian Data Protection Authority), Big Data: Privacy Principles Under Pressure (2013).

[68] French Autorité de la Concurrence & German Bundeskartellamt, Competition Law and Data Report, at 26 (May 10, 2016); Competition Bureau Canada, Big Data and Innovation: Key Themes for Competition Policy in Canada (2018), https://www.competitionbureau.gc.ca/eic/site/cb-bc.nsf/eng/04342.html [*hereinafter* Competition Bureau Canada Big Data Report]; Singapore, Data: Engine for Growth *supra* note 14.

[69] Buttarelli, EDPS *supra* note 67 at 1.

[70] U.K. Info. Comm'r Off. & CMA, Competition and Data Protection in Digital Markets: A Joint Statement Between the CMA and the ICO (May 19, 2021) at 10 (noting that categorizations of how data is used to compete in the digital economy "are not always the same as the relevant definitions from data protection law, and can often include both personal and non-personal data.").

[71] *See, e.g.*, Austl. Competition & Consumer Comm'n, *Digital Platforms Inquiry: Final Report* (July 26, 2019), https://www.accc.gov.au/publications/digital-platforms-inquiry-final-report [*hereinafter* ACCC Digital Platforms Inquiry Final Report]; U.K. Competition & Markets Auth.(CMA), *Online Platforms and Digital Advertising Market Study*, at 396 (July 1, 2020), https://www.gov.uk/cma-cases/online-platforms-and-digital-advertising-market-study.

Selection of Jurisdictions with Both Efficiency and Distributional Goals, above. For example, though EU competition law includes objectives around economic efficiency[72] and promoting overall competition,[73] the legislation also emphasizes "fair" competition. The European Commission explains that, while competition policy strives for classic economic efficiency goals like "better quality goods and services at lower prices," it is also "about applying rules to make sure companies compete fairly with each other."[74] The inclusion of such distributional goals is a significant difference from efficiency-only jurisdictions like the U.S., where antitrust law seeks to achieve only consumer welfare through competition, rather than the fair treatment of businesses.[75] In the U.S., fairness considerations are often the focus of consumer protection law, not antitrust.

Like some competition laws, data privacy law also emphasizes fairness as an objective.[76] Recent data privacy cases have considered the parameters of what constitutes "fair" data processing.[77] The U.K. privacy authority, for example, found that WhatsApp had failed to provide adequate and fair information on data processing to users in its plan to share data with Facebook after the companies merged.[78] The concept of fairness thus has some shared role in the legislative objectives of both realms, though data privacy law is interested in fairness in data processing, rather than fairness in competition.

Perhaps reflecting this commonality, the jurisdiction that has been most active in integrating data privacy into competition law, Germany, is also most active in enforcement of fairness-related

---

[72] Eur. Comm'n, Communication from the Commission: Guidance on the Commission's Enforcement Priorities in Applying Art. 82 [now 102] of the EC Treaty to Abusive Exclusionary Conduct Abusive Exclusionary Conduct by Dominant Undertaking, Dominant Undertakings, 2009 O.J. (L 2009/C 45/02), at ¶ 5 (explaining that the Commission "will direct its enforcement to ensuring that markets function properly and that consumers benefit from the efficiency and productivity which result from effective competition between undertakings.").

[73] Case No. C-501/06 P, GlaxoSmithKline Services Unlimited v. Comm'n and Others, E.C.R. I-9291, at ¶ 63 (2009).

[74] Eur. Comm'n, *Competition: Making Markets Work Better*, *supra* note 64 (emphasis added).

[75] Brown Shoe v. United States, 370 U.S. 294, 320 (1962) (the legislative history of antitrust law reveals "concern with the protection of competition, not competitors").

[76] *See, e.g.*, GDPR, *supra* note 30, at Art. 1(a) (" Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject."); PIPEDA, *supra* note 47, at § 4.4 ("Information shall be collected by fair and lawful means.").

[77] *See, e.g.*, Case C-645/19 Summary of the Request for a Preliminary Ruling Pursuant to Article 98(1) of the Rules of Procedure of the Court of Justice (2019) (summarizing the Belgian Commission on the Protection of Privacy case against Facebook, which included analysis of fairness of data processing in the first instance but was appealed on other, procedural grounds).

[78] Info. Comm'rs Office (U.K.), *Blog: A Win for the Data Protection of UK Consumers* (Mar. 14, 2018), https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2018/03/blog-a-win-for-the-data-protection-of-uk-consumers/.

competition law provisions. Germany has been unique in its pursuit of exploitative competition law abuses that involve data collection and privacy.[79] Exploitative theories of abuse center on extraction of excessive rents from consumers or businesses—in other words, they are fairness-based theories rather than the more common, efficiency-based violations of competition law.[80]

As the German example reflects, jurisdictions that emphasize fairness in their competition law (and perhaps more importantly, in their enforcement of that law) may have greater scope to incorporate data privacy considerations into their competition analysis. Though other factors likely influenced the appearance of privacy law in German competition enforcement (such as the strength of privacy interests in German law), the fairness goal opened the door to consideration of broader factors, like data privacy, within antitrust enforcement.

In contrast, jurisdictions like the U.S., which hews closer to a purely economic efficiency perspective, are more reticent to incorporate considerations of data privacy into antitrust law analysis. Their primary concern is that including considerations such as privacy within competition analysis will dilute or confuse the application of economic efficiency-based standards, making it unclear which factors should drive case or policy outcomes.[81] The goals of competition law in each jurisdiction may therefore influence the extent to which data privacy is considered, and incorporated into, competition policy and enforcement.

b. Free Movement of Data and the Promotion of Competition

As part of their data privacy legislative objectives, several jurisdictions emphasize the free movement of data. For example, the GDPR prevents restriction of "the free movement of personal data" within the European Union.[82] The Philippines privacy authority describes privacy

[79] *See* Figure 6. Case Study: The German Federal Cartel Office Case Against Facebook.

[80] *See* Part II.4.c Novel Theories of Exploitative Abuse: Dominance and Meaningful Consumer Consent to Data Collection.

[81] *See, e.g.,* Maureen K. Ohlhausen & Alexander P. Okuliar, *Competition, Consumer Protection, and The Right [Approach] to Privacy*, 80 ANTITRUST L.J. 1 (2015) (emphasizing the importance of separation between data privacy and antitrust to avoid confusing or diluting antitrust doctrine); Rod Sims, Address to the 2019 Competition Law Conference (May 25, 2019), https://www.accc.gov.au/speech/address-to-the-2019-competition-law-conference ("There is a strong push by some to broaden the objectives of competition law to address issues such as consumer privacy, economic inequality and even political influence. . . . Widening the objectives of competition law is likely to reduce its effectiveness. If we try to get competition law to achieve everything it may end up achieving nothing.").

[82] GDPR, *supra* note 30, at Art. 1 ("The free movement of personal data within the Union shall be neither restricted nor prohibited for reasons connected with the protection of natural persons with regard to the processing of personal data.").

legislation as "protect[ing] the privacy of individuals while ensuring free flow of information to promote innovation and growth."[83] Australia includes in its legislative objectives the "free flow of information across national borders," while still protecting individual privacy.[84] Since data movement can play a central role in enabling competition, such objectives of data privacy law are complementary with the policy objectives of competition law. This is particularly true in the digital economy, where data can be an important driver of competition. This is discussed further in the section of this Report on the shared policy interests of antitrust and data privacy in data portability.[85]

4. Shared Policy Interests and Concerns: Trust in Markets, Data Portability and the Impact of Demand-side Distortions in Consumer Choice

Despite having distinct enabling legislation and mandates, competition and data privacy authorities share a number of common policy interests. This section highlights three of the most prominent areas of shared attention: the promotion of trust in digital markets, data portability, and concern over demand-side distortions of consumer choice.

a. Promoting Trust in Digital Markets

Both antitrust and data privacy authorities emphasize the importance of trust in markets. There is a shared policy interest in fostering conditions that promote trust in markets, as a means of encouraging market participation.

Privacy agencies emphasize the building of trust between individuals and businesses (as well as government) within their mandates[86] and strategic priorities.[87] Some portray trust between

[83] Nat'l Privacy Comm'n, A Brief Primer on Republic Act 10173 – The Data Privacy Act of 2012, https://www.privacy.gov.ph/data-privacy-act-primer/ (describing the Philippine National Data Privacy Act).

[84] *The Privacy Act 1988,* No. 119, Part I, § 2A(a) (Austl.) ("The objects of this Act . . . [include] to facilitate the free flow of information across national borders while ensuring that the privacy of individuals is respected").

[85] *See* Part I.4.b. The Role of Data Portability in Enhancing Competition and Data Protection.

[86] *See, e.g.*, Personal Data Protection Comm'r of Singapore, *About Us*, https://www.pdpc.gov.sg/Who-We-Are/About-Us (mission includes "promot[ing] and enforc[ing] personal data protection so as to foster an environment of trust among businesses and consumers, contributing to a vibrant Singapore economy") (last visited May 12, 2021).

[87] Competition and Mkts. Auth., Corporate Report: Annual Plan 2020 to 2021 (Mar. 19, 2020), https://www.gov.uk/government/publications/competition-and-markets-authority-annual-plan-2020-to-2021/annual-plan-2020-to-2021 (strategic objectives include "[i]mproving trust in markets"); Off. of the Privacy Comm'r of Canada, *2018-2019 Annual Report to Parliament on the Privacy Act and the Personal Info. Protection and Elec.*

individuals and organizations as a fundamental part of the right to privacy.[88] Particularly in the digital economy, trust has been identified as the "lynchpin" of flourishing commerce.[89] Agencies describe the importance of building individual's trust that firms will process their data in accordance with data protection laws as a means to encourage consumer participation in markets, and a vibrant economy.[90] Conversely, violations of trust, in the form of misuse of personal information, data breaches and surveillance-based business models, leave consumers "wary of how the products and services on which they now depend for nearly all aspects of their activities are collecting and using their personal information."[91]

Competition authorities similarly emphasize the importance of trust and confidence in markets.[92] Consumer trust in businesses is seen as a precursor to the robust economic participation and

Documents Act 28 (2019) https://www.priv.gc.ca/en/opc-actions-and-decisions/ar_index/201819/ar_201819/ ("stress[ing] the need to promote trust and confidence in the digital economy").

[88] Info. Comm'rs Off. (U.K.), *Some Basic Concepts: What is Data Protection?*, https://ico.org.uk/for-organisations/guide-to-data-protection/introduction-to-data-protection/some-basic-concepts/ (last visited May 12, 2021) ("Data protection is the fair and proper use of information about people. It's part of the fundamental right to privacy –but on a more practical level, it's really about building trust between people and organisations."); Off. of the Privacy Comm'r of Canada, 2018-2019 Annual Report to Parliament, *id*. (proposing to amend the preamble of national privacy legislation to include "whereas privacy is essential to relations of mutual trust and confidence that are fundamental to the Canadian social fabric"); *See generally* Eur. Comm'n, Communication From the Commission to the European Parliament and the Council (July 24, 2019), https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52019DC0374&from=EN.

[89] Innovation, Science and Econ. Dev. Canada, Strengthening Privacy for the Digital Age: Proposals to Modernize the Personal Information Protection and Electronic Documents Act (May 21, 2019), https://www.ic.gc.ca/eic/site/062.nsf/eng/h_00107.html.

[90] Daniel Therrien, Privacy Comm'r of Canada, Remarks at the Univ. of Ottawa's Centre for Law, Tech. and Soc'y, A Data Privacy Day Conversation with Canada's Privacy Comm'r (Jan. 28, 2020) https://www.priv.gc.ca/en/opc-news/speeches/2020/sp-d_20200128/ ("a strong and competitive economy is not sustainable without trust; and trust requires the effective protection of rights"); Personal Data Protection Comm'n of Singapore, *About Us*, *supra* note 86 (emphasizing that data protection law enforcement creates trust, which contributes "to a vibrant Singapore economy."); U.K. Info. Comm'r Off. & CMA, Competition and Data Protection in Digital Markets: A Joint Statement Between the CMA and the ICO (May 19, 2021) at 19 (". . . giving individuals control over the use of their personal data can improve trust and confidence in the digital economy. . .").

[91] Innovation, Science and Econ. Dev. Canada, Strengthening Privacy for the Digital Age, *supra* note 89; U.K. Info. Comm'rs Office, Big Data and Data Protection Guide (July 2014) at 33 (observing that opacity in the processing of big data "can lead to a lack of trust that can affect people's perceptions of, and engagement with, the organisation doing the processing").

[92] Competition Bureau Canada, Big Data and Innovation: Implications for Competition Policy in Canada (2017) at 35, https://www.competitionbureau.gc.ca/eic/site/cb-bc.nsf/eng/04304.html ("The Bureau seeks to ensure that the advent of big data does not undermine the trust of consumers in the marketplace."); FTC, *Protecting Consumer Privacy and Security*, https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy-security (last visited May 10, 2021)("The agency uses law enforcement, policy initiatives, and consumer and business education to protect consumers' personal information and ensure that they have the confidence to take advantage of the many benefits of the ever-changing marketplace."); Andrea Coscelli, Chief Executive, Competition & Markets Auth., Key Address at the Fordham Competition Law Institute Conference: Regulation and Competition Enforcement–A

competition that drives consumer welfare.[93] Conversely, where there are trust-eroding market conditions—such as information asymmetries, a lack of transparency in pricing practices or anticompetitive conduct—this reduces consumer trust, confidence and engagement in the market.[94] Consumers lose out on benefits of using products and services as a result of their non-participation. Given this perceived importance, competition authorities have included measures aimed at improving consumer trust in recent proposals for regulation of digital platforms.[95]

This shared emphasis on trust in both competition and data privacy has even been framed as dynamically related. A 2019 U.K. report from a panel of digital competition experts, *Unlocking Digital Competition* (the Furman Report on Digital Competition), explains that "[a] trustworthy data protection system can, however, become an enabler of innovation and competition by giving consumers the trust and confidence to use new services."[96]

Antitrust and data privacy authorities have both examined similar market conduct that may reduce consumer trust, including the use of personalized pricing and algorithmic decision-making. Personalized pricing is generally understood as charging (or advertising) different prices

Combined Approach (Sept. 7, 2018) https://www.gov.uk/government/speeches/fordham-competition-law-institute-annual-conference-2018-keynote-speech.

[93] Coscelli, *supra* note 92 ("Consumers drive competition when they have the ability and confidence to exercise informed choices. This is particularly the case in digital commerce, where new business models that could benefit consumers will only grow if they are trusted and used by consumers."); FTC, *Protecting Consumer Privacy and Security*, *supra* note 92.

[94] *See e.g.* Competition & Markets Auth., *Online Platforms and Digital Advertising Market Study*, at 396 (July 1, 2020), https://www.gov.uk/cma-cases/online-platforms-and-digital-advertising-market-study [*hereinafter* CMA Online Platforms and Digital Advertising Market Study] ("Many of the concerns we have identified in digital advertising arise from, or are facilitated by, a lack of transparency and information asymmetries, leading in turn to a lack of trust"); *id*. at 345 ("In the [digital platform] markets we have reviewed, many decisions are taken by algorithms that are complicated and difficult for users to understand or scrutinise. As a result, users may lack sufficient information to make informed choices, undermining the effectiveness of competition. Users may also be influenced by choice architecture and default settings into taking choices that may not be in their best interests. All of these factors can reduce trust in the market."); ACCC Digital Platforms Inquiry Final Report*, supra* note 71 at 403 (finding that information asymmetries may cause "consumers not engaging in beneficial relationships with digital platforms because they do not have sufficient information to enable trust in digital platforms' data practices"); Competition & Mkts. Auth., *Algorithms: How they can Reduce Competition and Harm Consumers* 1, 17 (Jan. 19, 2021) [*hereinafter* CMA Algorithms Report] ("Information asymmetries and lack of trust and confidence in the integrity of the operations of key algorithms can lead consumers and customers to stop participating in digital markets, for example quitting social media apps or stopping using Google.").

[95] *See, e.g.,* CMA Online Platforms and Digital Advertising Market Study, *supra* note 94, at 346 (proposing trust and transparency requirements as part of a new code of conduct for online platforms with "strategic market status").

[96] Jason Furman et. al., Report of the Digital Competition Expert Panel: Unlocking Digital Competition (U.K.), at 124 (Mar. 13, 2019) [*hereinafter* Furman Report on Digital Competition]; *see similarly* Daniel Therrien, Privacy Comm'r of Canada, *supra* note 94 ("[A] strong and competitive economy is not sustainable without trust; and trust requires the effective protection of [privacy] rights.").

to different consumers, based on the individual's perceived willingness to pay.[97] Personalized pricing has recognized potential benefits for consumers, and is not generally a violation of competition law.[98] However, the vast amounts of widely-available consumer data online have created greater potential for companies to engage in highly personalized pricing.[99] The U.K.'s Competition and Markets Authority (CMA) observes that, in theory, "personalised pricing could harm overall economic efficiency if it causes consumers to lose trust in online markets,"[100] though the CMA and other antitrust authorities have found little evidence that harmful price discrimination is occurring online.[101] The theoretical competition concern is that consumer trust may be negatively impacted where consumers are subjected to non-transparent use of such pricing, and there is a lack of alternative, non-personally priced suppliers to which consumers could switch.[102]

Personalized pricing is just one example of algorithmic decision-making, a broader category of market practices that have captured the attention of policy-makers, antitrust and data privacy authorities for their potential impacts on consumers.[103] Algorithmic decision-making has

[97] CMA Algorithms Report, *supra* note 94, at 7.

[98] ACCC, Digital Platform Services Inquiry-September 2020 Interim Report (Austl.), at 102 (Oct. 23, 2020) https://www.accc.gov.au/publications/serial-publications/digital-platform-services-inquiry-2020-2025/digital-platform-services-inquiry-september-2020-interim-report ("Personalised pricing has the potential to improve overall consumer welfare as, for example, it may result in firms reducing prices to consumers with a low willingness to pay, enabling efficient trades that may not have otherwise occurred. It can also benefit consumers where firms are able to target customers of other firms with more competitive price offers."); CMA Algorithms Report, *supra* note 94, at 8 (observing similarly that personalized pricing has the potential to benefit consumers and competitors).

[99] Singapore, Data: Engine for Growth *supra* note 14, at ¶ 3.13 (noting increased potential for price discrimination as data proliferates).

[100] *See, e.g.*, CMA Algorithms Report, *supra* note 94, at 8; ACCC Digital Platform Services Inquiry Interim Report (2020), *supra* note 98 (noting lack of transparency around personalized pricing could lead to loss of trust in digital markets).

[101] CMA Algorithms Report, *supra* note 94, at 8 (noting limited evidence that personalized price advertising is being used online); ACCC Digital Platform Services Inquiry Interim Report (2020), *supra* note 98 at 517 (noting limited evidence to date of personalized pricing online).

[102] CMA Algorithms Report, *supra* note 94, at 8 (noting that "[t]he conditions under which competition authorities might be concerned about personalised pricing include where there is insufficient competition (i.e. monopolist price discrimination), where personalised pricing is particularly complex or lacking transparency to consumers and/or where it is very costly for firms to implement."); ACCC Digital Platform Services Inquiry (2020), *supra* note 98, at 102 (heightened concern over harm from personalized pricing where consumers have few or no alternative suppliers to whom they could switch).

[103] *See, e.g.*, EDPS, Opinion 7/2015 Meeting the Challenges of Big Data: A Call for Transparency, User Control, Data Protection by Design and Accountability, at 8 (2015) (noting impacts of lack of transparency); Info. Comm'rs Office (U.K.), Big Data, Artificial Intelligence, Machine Learning and Data Protection, at 27 (2017) https://ico.org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf (same); Art. 29 Working Party, *Guidelines On Automated Individual Decision-Making and Profiling For The Purposes Of Regulation 2016/679*, at 9 (Oct. 3, 2017); Art. 29 Working Party, *Guidelines on Transparency Under Regulation 2016/679* (Nov. 29, 2017), http://ec.europa.eu/newsroom/just/document.cfm; ACCC Digital Platform Services

expanded in ubiquity and importance in the digital economy. Privacy authorities have expressed concern over the potential effects on consumers from a lack of transparency in algorithmic data processing. Such opacity may violate privacy law transparency obligations.[104] It may also contribute to other types of privacy law violations, for example, where there is a lack of clarity around algorithmic processing, such that individuals are not able to exercise control over, or provide meaningful consent to, the collection or use of their data.[105] Most relevant here, this opacity in decision-making may erode the trust of buyers and sellers, and reduce consumer engagement in online markets.[106]

b. The Role of Data Portability in Enhancing Competition and Data Protection

Data portability rights have become one of the most-emphasized areas of complementarity between data privacy law and competition policy. Several jurisdictions now have data protection laws that grant consumers data portability rights.[107] Such rights empower individuals to request

Inquiry Interim Report (2020), *supra* note 98, at 138 (noting lack of transparency in algorithmic decision making could contribute to potential for platforms to self-preference their own vertical businesses); Fed. Cartel Office (Bundeskartellamt) (Ger.) & The Competition Auth. (Autorité de la Concurrence) (Fr.), Algorithms and Competition (Nov. 2019), https://www.bundeskartellamt.de/SharedDocs/Publikation/EN/Berichte/Algorithms_and_Competition_Working-Paper.pdf?__blob=publicationFile&v=5; CMA Algorithms Report, *supra* note 94; Competition Bureau Canada Big Data Report *supra* note 68, at 9 (noting a "prominent question" in competition law has been the role of algorithms in conclusion).

[104] *See, e.g.*, GDPR, *supra* note 30, at Art. 5(1)(a) (right to lawful, fair and transparent data processing); GDPR, *id.* at Art. 12(1) (requiring the controller to provide data subjects with concise, transparent, intelligible and easily accessible information about the processing of their personal data).

[105] EDPS, *Opinion 7/2015 Meeting the Challenges of Big Data,* at 8 (Nov. 19, 2015) (noting a lack of transparency impacts the ability of individuals to exercise control and consent over data processing); Info. Comm'rs Office, *Big Data, Artificial Intelligence, Machine Learning and Data Protection, supra* note 103, at 27 (same).

[106] *See, e.g.*, ACCC Digital Platform Services Inquiry, *supra* note 98, at 138; Info. Comm'rs Off., *Big Data, Artificial Intelligence, Machine Learning and Data Protection, supra* note 103, at 27-28 (opacity in data processing may impact trust and engagement of consumers).

[107] *See, e.g.*, GDPR, *supra* note 30, at Art. 20 (right to data portability for personal data); *The California Consumer Privacy Act of 2018*, *supra* note 36, at 1798.100(d) (requiring personal information be provided in a portable format upon request from a consumer); Press Release, Austl. Competition & Consumer Comm'n, ACCC Welcomes Consumer Data Right (May 9, 2018) (in May 2018, the Australian government adopted a Consumer Data Right that entitles individuals to access their data and have it transferred, in certain sectors); *Personal Data Protection Act 2012* (amendment) Bill, (Nov. 2, 2020) (Sing.) (passing amendments to the Personal Data Protection Act 2012 (PDPA) to introduces new data portability rights); Personal Data Protection Comm'n of Singapore & Competition and Consumer Comm'n of Singapore, Discussion Paper on Data Portability ¶ 1.6 (Feb. 25, 2019) 6 (noting that several jurisdictions, such as Australia, the European Union, India, Japan, Philippines, New Zealand, the U.K. and certain U.S. states have either implemented or are considering introducing the right to data portability in their domestic laws).

that certain categories of their personal data be transferred from one service provider to another, and obligate service providers to enable such transfer.[108] Though sometimes analogized to the ability of consumers to transfer their existing phone number to a new phone service provider, modern data portability rights are more complex, and enable potentially more extensive movement of data.

Data portability rights vary by jurisdiction in their existence and scope. Some countries do not include data portability rights within their privacy laws.[109] Others, like the U.S., have state but not federal data portability rights. The content of the legislated rights also varies, and the rights are so new that their scope is often at the early stages of legal interpretation and understanding.[110] There is also a broader emphasis on data portability beyond legally conferred rights, in the form of industry self-regulatory initiatives.[111]

Both antitrust and privacy agencies frequently point to data portability as indicative of the complementarity between data privacy law and competition.[112] In announcing a recent workshop focused on data portability, the FTC explained that "Data portability may . . . promote competition by allowing new entrants to access data they otherwise would not have, enabling the

[108] Some jurisdictions also use the term "data mobility" to refer to a similar concept as data portability. Here, "data mobility" is used in the more general sense to include the movement of data, whether pursuant to data portability obligations, interoperability obligations or more broadly. *See* Innovation, Science and Econ. Dev. Canada, *Strengthening Privacy for the Digital Age: Proposals to Modernize the Personal Information Protection and Electronic Documents Act* (2019) https://www.ic.gc.ca/eic/site/062.nsf/eng/h_00107.html (explaining the term "data mobility").

[109] *See, e.g.*, Statutory Law 1266 of 2008 (Colom.); Statutory Law 1581 of 2012 (Colom.).

[110] *See, e.g.*, Jacques Crémer, Yves-Alexandre de Montjoye, & Heike Schweitzer, Eur. Comm'n, *Competition Policy for the Digital Era* 77 (Apr. 4, 2019) [*hereinafter* Crémer Report] (which data can be ported, and how often are questions now subject to interpretation under GDPR).

[111] *See, e.g.*, Data Transfer Project, https://datatransferproject.dev/ (last visited May 10, 2021), an open-source initiative to expand user control over their data.

[112] Press Release, FTC, *FTC Announces September 22 Workshop on Data Portability* (Mar. 31, 2020) (noting data portability can promote competition); Joaquín Almunia, Competition Comm'r, European Comm'n, Remarks on Competition and Personal Data Protection at the Privacy Platform Event: Competition and Privacy in Markets of Data (Nov. 26, 2012) http://europa.eu/rapid/press-release_SPEECH-12-860_en.htm http://europa.eu/rapid/press-release_SPEECH-12-860_en.htm ("portability of data is important for those markets where effective competition requires that customers can switch by taking their own data with them."); Giovanni Buttarelli, Address to the European Parliament's Privacy Platform: Privacy and Competition in the Digital Economy at 3 (Jan. 21, 2015) (noting potential for data portability to enhance competition); Personal Data Protection Comm'n of Singapore & Competition and Consumer Comm'n of Singapore, *Discussion Paper on Data Portability* ¶ 1.6 (Feb. 25, 2019) (noting "consumers potentially benefit from having individual rights to data portability while market competition is enhanced by the existence of such rights."); Rod Sims, Austl. Competition & Consumer Comm'n, *2018 Compliance & Enforcement Priorities* (Feb. 20, 2018) ("Data portability increases competition").

growth of competing platforms and services."[113] This reflects the most commonly articulated view on complementarity: that data portability rights make it easier and more likely that consumers will switch between data-driven services, which encourages competition.[114] In the absence of portability rights, consumers might hesitate to change services, as doing so would mean leaving their data behind with the prior service provider. Now, consumers may have a legal right to take certain personal information with them. This right to portability is thought to enable new competitive entry and expansion by making it easier for entrants to win over customers (and their data) from incumbent firms.

Since data portability rights are a new legal phenomenon, their impact on competition is still emerging. Although much less common than a description of complementarity, there is some agency acknowledgement of a countervailing possibility—that data portability rights may help to entrench incumbent digital platforms, or limit the ability of smaller firms to enter and expand in the face of regulation.[115] The precise way in which this would occur is not often articulated in agency materials, but an example might be if consumers were to port their data predominantly from startups over to large companies, rather than vice versa as tends to be assumed. This seems plausible given the acknowledged prevalence of network effects in many digital markets, which draw consumers to the companies that have more users. Acknowledgement that data portability could reduce competition tends to be mentioned in passing, and one report describes such an effect as seemingly "limited."[116]

Still, antitrust policy reports in the EU, U.K. and Australia[117] observe that there are limitations in the ability of data portability rights alone to ensure robust competition. For example, multiple jurisdictions observe that the data portability right in the European GDPR permits only certain types of individual information (volunteered and observed data, not inferred data) to be ported.[118] Further, GDPR data portability rights are so far understood to require only point in time

[113] Press Release, FTC, *FTC Announces September 22 Workshop on Data Portability (*Mar. 31, 2020).

[114] *Id.*

[115] Crémer Report, *supra* note 110, at 82-83 (noting some scholars have expressed concern that data portability would diminish competition from small firms and startups, but that the anticompetitive potential of data portability rights under GDPR "seems to be limited").

[116] *Id.*

[117] Furman Report on Digital Competition, *supra* note 96, at 68-69 (Mar. 13, 2019) (describing limits of GDPR data portability provisions in enabling competition); Crémer Report, *supra* note 110, at 9 ("[D]uties to ensure data access —and possibly data interoperability—may need to be imposed," but cautioning context will be important to determining whether data is truly indispensable to competition.); ACCC Digital Platforms Inquiry Final Report, *supra* note 71, at 30.

[118] Furman Report on Digital Competition, *supra* note 96, at 68-69 (describing GDPR limitations to include the right to port covering only to a subset of directly provided consumer data); Crémer Report, *supra* note 110, at 81.

transfers, not continuous data access.[119] Such limitations are read by antitrust authorities to mean that, although helpful for competition, data portability rights are likely not sufficient in scope to ensure robust data-driven competition. Competition, particularly digital competition, may require a greater degree of ongoing data access than data portability rights are designed to provide.[120]

The Australian Competition and Consumer Commission (the ACCC) is among the most skeptical that data portability rights, standing alone, could restore digital competition in the face of incumbent market power. In its study of social media and online search markets, the ACCC observes that there are "no other competing platforms" to which consumers could switch if data portability rights were granted.[121] Even if there were options available in the market, the ACCC expresses doubt that extensive switching would occur, reasoning that consumers have no impetus to switch to save money on what are often free or "zero-price" digital services.[122] The ACCC draws a contrast to banking, where data portability has been used successfully to restore competition, and where consumers are price-motivated to switch services.[123] See explanation in **Figure 2. Case Study: The U.K. Open Banking Initiative**, below. Finally, the ACCC notes that, data portability may not be able to reduce the network effects that create barriers to entry and expansion in social and search digital markets, at least in the short term.[124] For example, if a consumer ports their data to a new social media service, unless members of their network move as well, the user is unlikely to switch to the new service— though multi-homing may occur (meaning the consumer uses multiple different service providers for the same type of service).[125]

[119] Furman Report on Digital Competition, *supra* note 96, at 68-69 (describing limitations of GDPR as not requiring continuous, rather than discrete, data transfers); Crémer Report, *supra* note 110, at 83 (noting GDPR data portability rights "unlikely to include real time access").

[120] *See* Crémer Report, *supra* note 110, at 83-84 (noting data interoperability enables multi-homing and development of competing services, contrasting interoperability to data portability as a concept).

[121] ACCC Digital Platforms Inquiry Final Report, *supra* note 117, at 30 ("The ACCC considers that data portability is unlikely to have a significant effect on barriers to entry and expansion in certain digital platform markets in the short term. . . . ," but recognizing the benefits of data portability, such as the promotion of innovation and new services).

[122] The term "zero-price" has been popularized in preference over the term "free" in agency and scholarly discussion of the digital economy, to reflect that consumers often exchange data or attention for digital services.

[123] ACCC Digital Platforms Inquiry Final Report, *supra* note 71, at 30.

[124] *Id.* at 116.

[125] *Id.*

Figure 2. Case Study: The U.K. Open Banking Initiative

Beginning in 2014, the U.K.'s Competition and Markets Authority (CMA) launched an extensive market investigation into the retail banking sector.[126] The resulting report found a widespread lack of competition in the sector.[127] The CMA proposed extensive reforms to restore competition in retail banking, including a new "open banking" initiative that began in 2018.[128]

The open banking initiative required the adoption of common and open technical standards for data, security and application programming interface (APIs), data portability and data access requirements. When requested to do so by a consumer, financial services firms are required to share specific account information with third parties, in a standardized way. Regulated third parties, with customer consent, may access current account information or initiate payments.

Open banking seeks to provide individuals with secure access to their financial information, from the service provider of their choice. By enabling consumers to share their transaction data with third parties in a reliable and secure way, open banking enabled new market entry and new service offerings, which compete with (or complement) existing bank services. For example, consumers can now sign up for overdraft warnings, and can view all of their accounts from different banks within one application.

Though still new, the open banking initiative has been popular and influential. As of January 2020, the CMA reported that over 1 million consumers were using open banking services, from more than 200 service providers.[129] Open banking initiatives are being pursued by Australia, Brazil, Canada, Hong Kong, Israel, Japan, Malaysia, New Zealand, Singapore and Taiwan.[130] In the EU, a revised Payment Services Directive includes requirements that are similarly aimed at improving competition, consumer choice and security in payment services.

Though the U.K. open banking reforms were initiated in response to competition concerns, the solution emphasizes "put[ting] customers in charge of access to their banking data"[131] through data interoperability and portability, much like data portability rights in privacy law.[132] The U.K.'s work on open banking demonstrates the potential for complementarity between data-driven competition, data portability and interoperability obligations.

This thinking has led several antitrust agencies to look beyond data portability rights to consider more extensive models of data mobility, such as open standards[133] or interoperability, as potential routes to robust digital competition.[134] **See Figure 3. Differentiating Between Interoperability and Data Portability,** below, discussing the distinction between the concepts of data portability and interoperability. Interoperability has been emphasized as a means of promoting competition in sectors such as fintech,[135] banking (see **Figure 2. Case Study: The**

[126] Competition & Markets Auth., Retail Banking Market Investigation Final Report at i (Aug. 9, 2016) (describing CMA retail banking market investigation as beginning in 2014).

[127] *Id.*; Competition & Markets Auth., Making Banks Work Harder For You at 1 (Aug. 9, 2016), https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/544942/overview-of-the-banking-retail-market.pdf. (summarizing findings of the CMA market investigation on retail banking, including that the older and larger banks, which account for the majority of the retail banking market, were not competing to retain customers).

[128] *See* Competition & Markets Auth., *Retail Banking Market Investigation* (last visited May 8, 2021), https://www.gov.uk/cma-cases/review-of-banking-for-small-and-medium-sized-businesses-smes-in-the-uk (providing documentation on adopted remedies).

[129] Colin Garland, Competition & Markets Auth., *Big Changes in Retail Banking* (Feb. 20, 2020) https://competitionandmarkets.blog.gov.uk/2020/02/20/big-changes-in-retail-banking/.

[130] Bill Roberts, Competition & Markets Auth., *Celebrating the First Anniversary of Open Banking* (Jan. 11, 2019), https://competitionandmarkets.blog.gov.uk/2019/01/11/open-banking-anniversary/. Jurisdictions such as Brazil have also pursued abuse of dominance cases against individual banks that refuse to permit access to consumer financial data. *See* OECD, Global Forum on Competition, Abuse of Dominance In Digital Markets – Contribution from Brazil - Session II, at 3 (Dec. 8, 2020), https://one.oecd.org/document/DAF/COMP/GF/WD(2020)7/en/pdf (discussing Bradesco and Guiabolso Admin. Proceeding 08700.004201/2018-38 in which Bradesco, one of the largest Brazilian retail banks, agreed to data portability obligations after an investigation into the company's refusal to permit clients to share their financial data with Guiabolso's application, in a manner that limited competition).

[131] Alasdair Smith, CMA Inquiry Chair, Competition & Markets Auth., Speech at the BBA Retail Banking Conference on Competition and Open Banking (June 30, 2017)**,** https://www.gov.uk/government/speeches/alasdair-smith-on-competition-and-open-banking.

[132] *See, e.g.*, Crémer Report, *supra* note 110, at 81 ("[T]he right to data portability was introduced in order to strengthen the data subjects' control over 'their' data (GDPR, recital 68). In the context of this report, we focus on the *economic control* it gives the individual.") (emphasis added).

[133] Furman Report on Digital Competition, *supra* note 96, at 71-72 (discussing the role of publicly developed and available open standards in competition).

[134] *Id.* (recommending measures to increase interoperability to promote digital competition); ACCC Digital Platforms Inquiry Final Report, *supra* note 71, at 11 (noting interoperability and consumer data rights may both be ways to reduce barriers to competition with major digital platforms); CMA Online Platforms and Digital Advertising Market Study, *supra* note 94, at 24 (recommending that a proposed digital markets regulator have the power to mandate interoperability and third-party access to data).

[135] Competition Bureau Canada, Technology-Led Innovation in the Canadian Financial Services Sector a Market Study, at 36 (Dec. 2017), https://www.competitionbureau.gc.ca/eic/site/cb-bc.nsf/vwapj/FinTech-MarketStudy-December2017-Eng.pdf/$FILE/FinTech-MarketStudy-December2017-Eng.pdf (emphasizing that interoperability between fintech platforms can reduce barriers to entry, and "spur competition and innovation from competing payment systems or infrastructures, driving inter-network competition").

U.K. Open Banking Initiative) as well as energy and telecommunications.[136] This reflects that for antitrust law, the importance of data mobility to competition is not a new development, nor is it unique to the digital economy.[137] However, the expansion of data-driven online business models has brought about a renewed emphasis on the role of data movement in competition, and data portability rights may play a role in this.

Figure 3. Differentiating Between Interoperability and Data Portability

Interoperability and portability can be understood as distinct but related concepts, both of which may contribute to similar outcomes in a data-driven market. Interoperability is a technological interconnection that enables the flow of data or interoperation of functions. Interoperability for data has been described as akin to portability, "but with a continuous, potentially real-time, access to personal or machine user data."[138] Data portability rights are limited to personal data, whereas interoperability is not—though interoperability could also be used to enable personal data transmission. Portability rights are held by individuals (though companies bear the compliance obligation), while interoperability obligations are imposed on companies through mechanisms such as regulation[139] or antitrust enforcement. Antitrust law has imposed interoperability remedies in cases that long predate the current discussion of digital markets and data portability rights.[140]

This antitrust attention to data mobility—beyond that afforded by data portability rights—also reflects the distinct mandates of antitrust and data privacy agencies. Despite the shared sense that

[136] Dep't for Business, Energy & Indus. Strategy & Dep't for Dig., Culture, Media & Sport (U.K.), Policy Paper, Smart Data Review: Terms of Reference (June 11, 2019), https://www.gov.uk/government/publications/smart-data-review/smart-data-review-terms-of-reference (review considering the role of data and access to it in financial services, energy and telecommunications markets).

[137] *See, e.g.*, Press Release, U.S. Dep't of Justice, *Justice Dep't Requires Ticketmaster Inc. to Make Significant Changes to Its Merger with Live Nation Inc.* (Jan. 25, 2010) (requiring as a condition of the Ticketmaster/Live Nation merger that clients of the merged firm be allowed to move a copy of their ticketing data with them should they move to a competing ticketing service). See also Part II. 4. Data Privacy Considerations in Abuse of Dominance/Monopolization Analysis.

[138] Crémer Report, *supra* note 110, at 58.

[139] The Payment Services Directive 2015/2366, which effectively requires interoperability, is an example of a more extensive regulatory intervention. PSD2-directive (Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on Payment Services in the Internal Market, O.J. (L 337)).

[140] United States v. Microsoft Corp., 253 F.3d. 34, 99-100 (D.C. Cir. 2001); United States v. Microsoft, No. 98-1232 (CKK) (D.D.C. Nov. 12, 2002) at *1, modified and superseded (Sept. 7, 2006), further modified and superseded, 2009 WL 1348218 (Apr. 22, 2009). *See, e.g.*, Case No. T-201/04, Microsoft/Windows Media Player, E.C.R. (2007) (Microsoft abused its dominance through a refusal to supply interoperability information and technical tying of products).

data portability rights are positive for competition, those rights have differing relevance to each area of law. Privacy agencies and privacy law emphasize portability for its benefits to individuals, as part of a suite of privacy rights and interests held by data subjects. Data portability obligations are enforced as a means to provide data control and autonomy to individuals, in conjunction with other privacy rights, such as the right to deletion or the right to be forgotten. For data privacy agencies, competition is largely a byproduct, rather than the purpose, of data portability rights.[141] For antitrust agencies, data portability is relevant only to the extent it impacts competition, not because of any normative importance of data privacy law. The antitrust agency perspective tends to be that data portability rights are a positive, but not necessarily adequate, means of advancing their mandates to promote competition.

c. Consumer Choice and the Challenges of Demand-Side Distortions

Antitrust and data privacy authorities share a policy interest in promoting consumer choice, and mutual concern over impediments to such choice. As the U.K. competition and data privacy authorities observe, "meaningful user choice and control are fundamental both to robust data protection and effective competition."[142] The acting head of the FTC similarly observes that for data-driven services, the "dearth of real [consumer] choice is a privacy problem, but it is also a competition problem."[143]

Both privacy and competition law often seek to promote consumer choice in markets, although for different reasons. Consumer choice, often in the form of notice and consent, has long been a central principle within privacy law.[144] In privacy policies or other representations, companies

[141] *See, e.g.*, Furman Report on Digital Competition, *supra* note 96, at 68 (noting competition is, understandably, not a key objective of data portability regulations or regulators).

[142] U.K. Info. Comm'r Off. & CMA, Competition and Data Protection in Digital Markets: A Joint Statement Between the CMA and the ICO (May 19, 2021) at 19.

[143] FTC, *Hearings on Competition and Consumer Protection in the 21st Century, Hearing No. 12: The FTC's Approach To Consumer Privacy* 131 (Apr. 10, 2019) (remarks by FTC Commissioner Rebecca Kelly Slaughter).

[144] *See, e.g.*, GDPR *supra* note 30, at Art. 6(1)(a) (consent of the data subject is a ground for lawful data processing); U.S. Dep't of Health, Educ., & Welfare, Report of The Secretary's Advisory Committee on Automated Personal Data Systems, Records, Computers, and the Rights of Citizens (July 1973) (first articulation of the Fair Information Privacy Practices (FIPPS) emphasizing notice and consent); Children's Online Privacy Protection Rule §312.5, 15 U.S.C. §6501 (2013) (requiring verifiable parental consent to be obtained by the covered entities that collect the personal information of children under 13); Off. of the Australian Info. Comm'r (OAIC), *Digital Platforms Inquiry–Submission to the Australian Competition and Consumer Commission* (Apr. 17, 2018) https://www.oaic.gov.au/engage-with-us/submissions/digital-platforms-inquiry-submission-to-the-australian-competition-and-consumer-commission/ ("Central themes in the Privacy Act—such as transparency, choice and control for individuals and accountability . . . are intended to support individuals in making decisions about their personal information"); Off. of the Privacy Comm'r of Canada, Policy and Research Group, *A Discussion Paper Exploring Potential Enhancements to Consent Under the Personal Information Protection and Electronic*

provide notice describing how the personal data of individuals will be collected, used, shared, sold or otherwise processed.[145] Individuals then choose whether or not to provide their consent for the data-related activities that have been described.[146] Privacy legislation around the globe emphasizes this type of privacy self-management by consumers.

Though more often the focus of consumer protection law, consumer choice is also relevant to competition law. Competition in markets drives the creation of a range of product and service choices for consumers.[147] Antitrust law seeks to combat anticompetitive conduct and mergers, both of which can reduce consumer choice in markets.[148]

Given the consumer choice emphasis in both legal regimes, there is a shared concern over the potential effect on choice arising from consumer behavioral biases, information asymmetry and limited or complex offerings of privacy choice. Collectively termed "demand-side distortions" here, these and other market phenomena may impact consumers' ability to exercise choice to their own benefit, particularly in the digital economy. The descriptions of such impacts are extensive and varied in agency materials, but the following are often identified as impairing consumers' ability to make informed privacy choices in digital markets:

- **Information asymmetry:** Competition and privacy authorities share the concern that consumers have low awareness of how their personal data is being collected and used, and the reality and extent of data processing by many commonly used

Documents Act, at 1 (May 2016), https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2016/consent_201605/ [*hereinafter* OPC Consent Report 2016] (describing consent as "the cornerstone" of Canada's federal private sector privacy law).

[145] *See e.g.*, OPC Consent Report 2016 *supra* note 144, at 2-3 (describing the operation of Canadian federal privacy law, *Personal Information Protection and Electronic Documents Act* (PIPEDA), S.C. 2000, c.5, as relying "on knowledge and consent as a requirement for the collection, use and disclosure of personal information. Organizations are required to inform individuals about what personal information they will collect, how they plan to use or disclose that information, and for what purposes, to enable individuals to decide whether or not to provide consent," although noting the legislation includes certain exceptions to the notice and consent requirements).

[146] *See e.g.* GDPR*, supra* note 30, at Art. 6(1)(a) (consent of the data subject is a ground for lawful data processing)

[147] *See, e.g.*, *The Philippine Competition Act* (R.A. 10667), s. 2 ("Unencumbered market competition also serves the interest of consumers by allowing them to exercise their right of choice over goods and services offered in the market."); Eur. Comm'n, *Competition Policy*, https://ec.europa.eu/competition/general/overview_en.html (last visited May 8, 2021) (noting competition policy in Europe "creates a wider choice for consumers").

[148] *See, e.g.*, FTC, *What We Do*, https://www.ftc.gov/about-ftc/what-we-do (last visited May 8, 2021) ("The FTC will challenge anticompetitive mergers and business practices that could harm consumers by resulting in higher prices, lower quality, *fewer choices*, or reduced rates of innovation."); Paul Nihoul, *"Freedom Of Choice": The Emergence Of A Powerful Concept In European Competition Law*, CHOICE: A NEW STANDARD FOR COMPETITION ANALYSIS?, CONCURRENCES REVIEW, 10-21 (Paul Nihoul et. al. ed., 2016) (tracing the role of consumer choice considerations in EU competition decisions).

services.[149] The challenge of information asymmetry is expressed in many different ways and contexts, but often includes recognition of consumers' well-documented tendency not to read what have become long, complex and ubiquitous terms and conditions of service before purporting to consent to those terms.[150] In fact, agencies recognize the reality that, given the "often incompressible policies" that regularly change, it may be unfair to expect consumers to make meaningful decisions about consent.[151]

Even consumers who try to engage with the terms of service may find that, at the moment of consent, it is difficult to understand the extent and variation of potential uses of their data that will occur within the digital ecosystem.[152] The Australian competition authority observes that "few consumers are fully informed of, fully understand, or effectively control, the scope of data collected and the bargain they are entering into with digital platforms when they sign up for, or use,

[149] *See, e.g.*, Info. Comm'rs Office (U.K.), Investigation into Data Protection Compliance in the Direct Marketing Data Broking Sector, at 25 (Oct. 2020), https://ico.org.uk/media/action-weve-taken/2618470/investigation-into-data-protection-compliance-in-the-direct-marketing-data-broking-sector.pdf (finding low public awareness and lack of clarity on the use of their personal data by data brokers); Preliminary Opinion of the EDPS, Privacy and Competitiveness in the Age of Big Data: the Interplay between Data Protection, Competition Law and Consumer Protection in the Digital Economy 34-35 (Mar. 2014) (discussing information asymmetries as a barrier to genuine consumer choice regarding privacy protection); Off. of the Privacy Comm'r of Canada, 2016-17 Annual Report to Parliament on the *Personal Information Protection and Electronic Documents Act* and the *Privacy Act* 17 (Sept. 2017), https://www.priv.gc.ca/media/4586/opc-ar-2016-2017_eng-final.pdf ("…complex information flows, and business processes involving a multitude of third-party intermediaries, such as search engines, platforms and advertising companies, have put a strain on the consent model. In this age of big data, the Internet of Things, artificial intelligence and robotics, it is no longer entirely clear to consumers who is processing their data and for what purposes.").

[150] *See, e.g.*, Innovation, Science and Econ. Dev. Canada, *Strengthening Privacy for the Digital Age: Proposals to Modernize the Personal Information Protection and Electronic Documents Act* (2019) https://www.ic.gc.ca/eic/site/062.nsf/eng/h_00107.html ("Although many organizations have privacy policies in place, these are notoriously long and complex to understand, and most individuals neither have time nor sufficient legal training to understand them").

[151] Off. of the Privacy Comm'r of Canada, 2016-2017 Annual Report to Parliament on the *Personal Information Protection and Electronic Documents Act* and the *Privacy Act* 11 (Sept. 2017), https://www.priv.gc.ca/media/4586/opc-ar-2016-2017_eng-final.pdf (". . . where efforts to explain privacy practices tend to take the form of long, legalistic and often incomprehensible policies and terms of use agreements that are constantly evolving, it is unfair to expect individuals to be able to exert any real control over their personal information or to always make meaningful decisions about consent.").

[152] *See, e.g.*, Innovation, Science and Econ. Dev. Canada, *supra* note 150 ("The multiplicity of online interactions can present challenges to individuals to understand the nature and extent of information sharing that occurs in this environment.").

their services."[153] This inability to understand the scope of data processing can make it difficult for consumers to assess elements of privacy quality, such as the level of protection that will be afforded to their data.

- **Consumer biases:** Relatedly, there is concern that consumer behavioral biases may influence the process and outcomes of consumer choice, particularly in digital markets. A wide variety of behavioral biases are well-documented throughout privacy research and agency materials, including:

    - The privacy paradox: many studies have suggested that consumers' stated value preference for strong privacy protection is not consistent with their revealed preference.[154] Despite declaring that privacy is important, in specific contexts consumers then often demonstrate a willingness to give up personal data in exchange for minimal reward.

    - Inertia bias: consumers tend to continue to use existing products, even when the quality declines, and tend to accept default settings for data processing;[155] and

    - The effect of "free" products or services: consumers tend to overvalue products that have a price of zero dollars. Many digital services do not charge a price to the consumer-facing side of the platform.

  Scholars have suggested that individuals' privacy decisions are influenced by factors such as the uncertain nature of privacy trade-offs, the context in which a

[153] ACCC Digital Platforms Inquiry Final Report (2019), *supra* note 71, at 2; OPC Consent Report 2016, supra note 150 at 6 ("Binary one-time consent is being increasingly challenged [in the digital environment] because it reflects a decision at a moment in time, under specific circumstances, and is tied to the original context for the decision . . .").

[154] *See, e.g.*, OPC Consent Report 2016, *supra* note 144 at 9(observing "[m]any studies have found that people who say they care about privacy at the same time may disclose vast amounts of personal information online." and canvassing several such studies); Leslie John, *We Say We Want Privacy Online, But Our Actions Say Otherwise*, Harvard Business Review (Oct. 16, 2015) https://hbr.org/2015/10/we-say-we-want-privacy-online-but-our-actions-say-otherwise; Daniel J. Solove, *The Myth of the Privacy Paradox*, 89 GEORGE WASH. L. R. 1 (2021) (arguing that the widely-acknowledged privacy paradox is a myth, created by faulty logic that compares general attitudes about privacy to context-specific privacy risk decisions).

[155] *See, e.g.*, ACCC Digital Platforms Inquiry Final Report, *supra* note 71, at 110 (noting barriers created by customer inertia in changing default search settings, which advantages Google as the most prevalent default search engine installed on desktop, mobile and other devices).

privacy decision is being made and malleability/susceptibility to manipulation by commercial or government interests.[156]

- **Limited choice or complex choice:** Even when consumers actively seek to protect their data privacy, the ways in which privacy options are presented for digital services may be complex or misleading. The "choices" are being provided to consumers in a manner that precludes the exercise of meaningful consent.

  Particularly in the digital context, there is concern from both privacy and competition authorities that services, and privacy disclosures, are being designed to exploit consumer behavioral biases.[157] Recent Norwegian California regulations,[158] and an FTC workshop, [159] have addressed "dark patterns," which are described as deceptive or manipulative user interface designs that push consumers to take "unintended actions that may not be in their interest."[160] Similarly, the U.K. competition and data privacy agencies have examined the role of "choice architecture" on users' ability to make informed choices about the processing of their personal data.[161] This tends to be predominantly a privacy or consumer protection concern,[162] but it has also been viewed as problematic for competition where there are few alternatives available in the market, and existing services require consumers to consent to data processing as a condition of use.[163]

[156] *See, e.g.*, Allesandro Acquisti, Laura Brandimarte, George Loewenstein, *Privacy and Human Behavior in the Age of Information*, 347 SCIENCE 509, 509-514 (2015).

[157] *See, e.g.*, CMA Algorithms Report, , *supra* note 94, at 6 (discussing the role of algorithms in online choice architecture, including consumer susceptibility to default options, limited attention spans, loss aversion and inertia to change).

[158] The California Consumer Privacy Act of 2018, CAL. CIV. CODE § 999.306.

[159] Press Release, FTC, *Bringing Dark Patterns to Light: An FTC Workshop*, Apr. 29, 2021 https://www.ftc.gov/news-events/events-calendar/bringing-dark-patterns-light-ftc-workshop

[160] Transcript, Bringing Dark Patterns to Light: An FTC Workshop, Apr. 29, 2021 at 1 (introductory comments of FTC Commissioner Rebecca Kelley Slaughter), https://www.ftc.gov/system/files/documents/public_events/1586943/ftc_darkpatterns_workshop_transcript.pdf; *See also* Norwegian Consumer Council (Forbrukerrådet), *Deceived by Design: How Tech Companies use Dark Patterns to Discourage Us from Exercising Our Rights to Privacy* (June 27, 2018).

[161] U.K. Info. Comm'r Off. & CMA, Competition and Data Protection in Digital Markets: A Joint Statement Between the CMA and the ICO (May 19, 2021) at 21.

[162] *See, e.g.*, Norwegian Consumer Council (Forbrukerrådet), *Deceived by Design: How Tech Companies use Dark Patterns to Discourage Us from Exercising Our Rights to Privacy* (June 27, 2018) (observing that digital platforms design user interfaces to push users toward more privacy-invasive options).

[163] Part II.4.c.i. Dominant Firms with "Take it or Leave it" Data Collection Terms of Service.

> A lack of choice means consumers who seek to protect their data privacy may still be unable to effectively do so. [164]

Privacy authorities are considering these and other demand-side distortions because they present significant questions about the limitations of notice and consent.[165] Do notice and consent models effectively protect consumer data privacy interests, even in the face of consumer bias and information asymmetry? The OECD observes that:[166]

> The inability of consumers to engage with privacy policies, and behavioural biases limiting consumers' ability to meaningfully engage with privacy policies may result in consumers agreeing to policies that they do not actually agree with. Such outcomes could undermine the effectiveness of data protection laws that rely predominately on consumer consent to ensure good data protection outcomes.

From a competition perspective, such demand-side distortions are also of interest, because they may mean consumer decision-making does not play its usually-assumed role in disciplining firm behavior.[167] In well-functioning markets, businesses innovate and compete to attract consumers. Competition drives businesses to offer consumers choices. Competition law generally assumes that consumers are able to make informed choices between the products and services offered by those businesses, based on factors like price, innovation, service and quality.[168] The expectation tends to be that, in competitive markets, consumer decision-making will discipline weak or bad actors in a market, as consumers move their business and data to firms that provide the desired combination of features in their product or service offerings.

---

[164] CMA Online Platforms and Digital Advertising Market Study, *supra* note 94, at 181 ("[i]f there were more choice for consumers, then there could be scope for more competition between platforms as platforms would need to compete more actively to persuade consumers of the benefits of personalised advertising. There would also be scope for other platforms to compete for consumers on the basis of alternative business models offering different options in respect of the privacy choices and the services that they offer.").

[165] *See, e.g.*, FTC, *Hearings on Competition and Consumer Protection in the 21st Century, Hearing No. 12: The FTC's Approach To Consumer Privacy* 131 (Apr. 10, 2019) (remarks by FTC Commissioner Rebecca Kelly Slaughter) (describing the limitations of notice and consent as a subject that raises concerns about both competition and privacy).

[166] OECD, Consumer Data Rights and Competition – Background Note, *supra* note 6, at 35.

[167] *See, e.g.*, OECD, Zero-Price Markets – Background Note, *supra* note 9, at 24 (discussion of competitive impact potentially arising from demand-side distortions in zero-price markets).

[168] *See, e.g.*, Danish Competition and Consumer Authority, *Strategy and Values*, https://www.en.kfst.dk/about-us/strategy-and-values/ (last visited May 8, 2021) ("In a well-functioning market, companies compete effectively with each other, for both private and public contracts, while consumers make informed choices and are active in the market.").

In theory, similar assumptions might also apply where there is competition based on privacy quality—that consumers would switch to products and services that offer the desired level of privacy protection, leaving those businesses that fail to do so. However, the OECD observes that information asymmetries and the other distortions discussed above may leave consumers unable or unwilling to assess the true privacy quality of products and services in their decision-making processes.[169] Consumers may not know that businesses are misusing their data, or they may be otherwise unable (or unwilling) to take action to control how their data is being used. As a result, consumers may not be in a position to make effective privacy choices that promote optimal privacy levels or discipline privacy bad actors.[170] The result may be sub-optimal privacy competition—less consumer demand for privacy controls leads to reduced competition among firms to provide these controls,[171] such that competition alone cannot be relied upon to drive optimal levels of privacy. One agency describes this as a market failure that prevents the efficient operation of demand for the privacy dimensions of products and services.[172]

These privacy demand distortions may affect antitrust analysis. A 2019 expert report to the European Commission, Competition Policy for the Digital Era (the "Crémer Report"), notes that such distortions ought to be taken into account in the evaluation of market power and anticompetitive effects.[173] It suggests, for example, that consumer biases may make it less likely that consumers will switch services, even in the face of declining quality. This could cushion incumbents against competition by allowing them to retain customers even if they have lower-quality service offerings. Some agencies go further, suggesting that incumbent firms are purposefully exploiting consumer biases, and information asymmetries, to marginalize rivals and reduce competition in digital markets.[174]

Demand-side distortions in consumer choice may even impact how competition and privacy are understood to interact. Antitrust authorities have relied on an expectation that data privacy law would mitigate or constrain data related effects on competition that are otherwise likely to arise

[169] OECD, Consumer Data Rights and Competition – Background Note, *supra* note 9, at 2 ("Effective competition should theoretically drive better outcomes for consumers in terms of higher levels of privacy and control of personal data. However, it is not clear this is always the case, especially where consumers do not engage with consumer data rights, perhaps because of behavioural biases or a perceived lack of options.").

[170] *Id.*

[171] *Id.*

[172] ACCC Digital Platforms Inquiry Final Report, *supra* note 71, at 403.

[173] *See, e.g.*, Crémer Report, *supra* note 110, at 50 (concurring with professor Fiona Scott Morton's comments to this effect).

[174] *See, e.g.*, CMA Algorithms Report, *supra* note 94, at 6. *See also* Part II. 4. Data Privacy Considerations in Abuse of Dominance/Monopolization Analysis.

from mergers.[175] However, as the OECD explains, "[demand-side distortions] may undermine the effectiveness of consent-based models of data protection, some of which competition agencies have relied on to promote good outcomes in respect of data protection where a merger or market power may have otherwise undermined such outcomes."[176] In other words, the strength of this assumption—that data privacy law will mitigate anticompetitive effects—may be eroded where demand-side distortions impact the effectiveness of privacy protection that is reliant on consumer self-management.

Ultimately, such demand-side issues present a shared dilemma for competition, privacy and also consumer protection law. As the OECD observes: "In many cases, demand-side market problems in digital zero-price markets cannot be neatly categorised into competition, consumer protection . . . As a result, regulatory cooperation and the development of coordinated solutions may be particularly important."[177]

Part II: Theory and Practice at the Intersection of Antitrust and Data Privacy

This Part considers the emerging theory and practice at the intersection of antitrust and data privacy law. It introduces the leading theory of how antitrust law ought to account for data privacy, which posits that antitrust analysis should consider privacy only when it is a parameter of product or service quality in the relevant market. It then considers the practical challenges of analyzing privacy quality as it relates to competition.

Building on this introduction to the privacy-as-quality theory, the remainder of this Part explores the relevance of data privacy to several major areas of antitrust law: market definition and market power, merger review, abuse of dominance, cartels/competitor collaborations and remedies.

1. Integrating Data Privacy into Antitrust Analysis: The "Privacy-as-Quality" Theory

The leading theory on the interaction between antitrust law and data privacy posits that antitrust analysis should consider privacy when it is an element of product or service quality that is affected by competition. Where companies compete to offer privacy products or features to consumers in a market, privacy may be a factor in the antitrust analysis. This "privacy-as-

[175] *See* Part II. 3. Data Privacy Considerations in Merger Review.

[176] OECD, Consumer Data Rights and Competition – Background Note *supra* note 6, at 36.

[177] OECD, Zero-Price Markets – Background Note, *supra* note 9, at 24 (commenting on the importance of regulatory cooperation in zero-price markets given demand distortions).

quality" theory accounts for increases or decreases in privacy, when—and only when—privacy is a parameter of quality that is affected by competition in the relevant market.

For example, certain internet browsers and mobile device companies have positioned themselves in the marketplace as offering stronger privacy protection and features than their rivals. Consumers may choose those browsers, or that particular mobile device, over competing options because of the superior personal data protection they offer. If those companies became involved in a merger review or were accused of antitrust misconduct, the antitrust analysis would include consideration of any likely effects on privacy-based competition caused by that merger (or misconduct) in the relevant market.

The U.S. Department of Justice, Antitrust Division (DOJ Antitrust Division) monopolization case against Google provides a recent example of alleged privacy quality effects.[178] The complaint claims that "[b]y restricting competition in search, Google's conduct has harmed consumers by reducing the quality of search (including on dimensions such as privacy, data protection, and use of consumer data) . . . ."[179] Conversely, where conduct or a merger is found to likely to encourage or increase privacy-based competition and quality, that would be viewed as a positive factor in the antitrust assessment.

This "privacy-as-quality" view is the most widely articulated, and the most developed, theory of the relationship between data privacy and potential antitrust harm.[180] Though far from settled in its theory or application, this conception of privacy as quality has drawn more acknowledgement

[178] Press Release, U.S. Dep't of Justice, *Justice Department Sues Monopolist Google for Violating Antitrust Laws* (Oct. 20, 2020), https://www.justice.gov/opa/pr/justice-department-sues-monopolist-google-violating-antitrust-laws (emphasis added); *see also* Complaint, State of New York v. Facebook, Inc., No. 1:20-cv-03589 (D.D.C. Dec. 9, 2020) (alleging that, once Facebook obtained monopoly power the company "degraded the privacy protections and privacy options" that had led to its initial popularity over social networking rivals).

[179] U.S. Dep't of Justice, *id.*

[180] Geoffrey A. Manne & R. Ben Sperry, *The Problems and Perils of Bootstrapping Privacy and Data into an Antitrust Framework*, CPI ANTITRUST CHRONICLE 1, 3-5 (May 2015) (disagreeing with the approach of privacy as quality, but acknowledging it is one of the most developed theories).

from antitrust agencies than any other theory. Agency speeches,[181] submissions,[182] and proposed guidance[183] in several jurisdictions have recognized that competition may be based on data protection or privacy as an element of product or service quality. Some jurisdictions have applied this theory in merger reviews and, more recently, abuse of dominance cases.[184] This view is the closest to consensus thinking, or at least the most widely referenced paradigm, at this intersection of antitrust law and data privacy.

At the same time, it remains quite new. The theory's full meaning, implications and potential applications are still at the early stages of understanding. In practice, much of the agency analysis of privacy quality has been concentrated in the context of merger reviews, with some very early application in abuse of dominance cases. These applications are discussed below, in sections of this Report specific to each type of conduct.[185] It is not yet clear how the concept of privacy as quality might be applied across other areas of antitrust law, such as market definition, market power or cartels, though in theory privacy could be considered an element of quality in those contexts as well. It is also not yet clear whether this privacy-as-quality theory will prove sufficiently broad or robust to address all of the interactions that are rapidly emerging between antitrust and data privacy law.

[181] Deborah Feinstein, Big Data in a Competition Environment, CPI ANTITRUST CHRONICLE at 1, 2 (May 2015) www.competitionpolicyinternational.com/assets/Uploads/FeinsteinMay-152.pdf ("[T]he FTC has explicitly recognized that privacy can be a non-price dimension of competition."); *See, e.g.*, Margrethe Vestager, Comm'r of Competition, Eur. Comm'n, Mackenzie Stuart Lecture at Cambridge: Making The Data Revolution Work For Us (Feb. 4, 2019) ("[I]f privacy is something that's important to consumers, competition should drive companies to offer better protection."); Noah Joshua Phillips, Comm'r, FTC, Should We Block This Merger? Some Thoughts on Converging Antitrust and Privacy, The Ctr. for Internet and Soc'y 3 (Jan. 30, 2020), ("Privacy can be evaluated as a qualitative parameter of competition, like any number of non-price dimensions of output."); Makan Delrahim, Asst. Att'y Gen., Dep't of Justice, Remarks for the Antitrust New Frontiers Conference "…And Justice for All": Antitrust Enforcement and Digital Gatekeepers (June 11, 2019) https://www.justice.gov/opa/speech/assistant-attorney-general-makan-delrahim-delivers-remarks-antitrust-new-frontiers ("[D]iminished quality is also a type of harm to competition. . . . [P]rivacy can be an important dimension of quality.").

[182] OECD, Consumer Data Rights and Competition – Note by Germany, at 4 (June 12, 2020), https://one.oecd.org/document/DAF/COMP/WD(2020)32/en/pdf ("[I]f customers have a choice regarding the control of their privacy level, privacy can become an important parameter of competition.")

[183] Competition & Consumer Comm'n of Singapore, *Proposed Amendments to the CCCS Guidelines*, Consultation Document at Annex D (Sep. 10, 2020), https://www.cccs.gov.sg/public-register-and-consultation/public-consultation-items/2020-public-consultation-on-proposed-changes-to-competition-guidelines (proposal to update merger guidance to "clarify that data protection can be an aspect of competition" that the competition authority may consider).

[184] Complaint, U.S. Dept. of Justice v. Google, No. 1:20-cv-03010 (D.D.C. Oct, 20, 2020); Complaint at ¶¶ 235-244, State of New York et al v. Facebook, Inc., No. 1:20-cv-03589 (D.D.C. Dec. 9, 2020).

[185] *See* Part II.3. Data Privacy Considerations in Merger Review and Part II.4. Data Privacy Considerations in Abuse of Dominance/Monopolization Analysis.

Data privacy authorities have described a similar view of privacy as an element of product quality and competition. The European Commission's two-year retrospective on the GDPR observes that "[m]any businesses also promote respect for personal data as a competitive differentiator and a selling point on the global marketplace, by offering innovative products and services with novel privacy or data security solutions."[186] Privacy agencies regularly reference and conduct research that suggests consumers place a growing emphasis on privacy as an element of product choice. For example, a survey by the Office of the Australian Information Commissioner (OAIC) found that privacy "is the leading consideration when choosing an app or program to download, ahead of quality, convenience and price, and 84% consider privacy extremely or very important when choosing a digital service."[187]

It is fair to note, however, that the OECD describes the privacy-as-quality view as "the subject of debate," because of perceived limits on consumers' ability to evaluate privacy quality as part of their decision making.[188] If biases, information asymmetries or other market realities limit the conscious ability of consumers to choose products and services that are consistent with their privacy preferences, this could reduce the relevance of privacy-based competition.[189] It would be helpful for antitrust and data privacy authorities to discuss and develop further clarity around whether and when privacy-based competition might be expected to impact the privacy features and quality of products in markets, particularly given the acknowledgement of both realms that demand-side distortions can affect consumers' privacy choices.

As it is currently understood, this privacy-as-quality theory plays both an integrating and a limiting role where privacy meets antitrust law. The theory incorporates data privacy into longstanding antitrust analytical frameworks, which recognize that quality may be the basis for

[186] Eur. Comm'n, *Communication from the Commission to the European Parliament and the Council: Data Protection as a Pillar of Citizens' Empowerment and the EU's Approach to the Digital Transition – Two Years of Application of the General Data Protection Regulation*, at 3 (June 24, 2020), https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020DC0264&from=EN; Peter Hustinx, Eur. Protection Supervisor, *Data Protection and Competition: Interfaces and Interaction, the Data Protection Law in the Context of Competition Law Investigations* (June 13, 2013) (similarly).

[187] Office of the Austl. Info. Comm'r, *Australians Want More Control Over Privacy, Survey Shows* (Sept. 24, 2020), https://www.oaic.gov.au/updates/news-and-media/australians-want-more-control-over-privacy-survey-shows/.

[188] OECD, Zero-Price Markets – Background Note, *supra* note 9, at 7 ("The concept [of privacy as quality-based competition] is nonetheless the subject of some debate, particularly with respect to whether consumers consciously consider privacy when making product decisions, and the degree to which firms' privacy offer responds to competitive pressure."). For further discussion of these demand-side distortions, see Part I.4.c. Consumer Choice and the Challenges of Demand-Side Distortions.

[189] OECD, *id.*

competition in markets.[190] This integration is achieved by interpreting the concept of "quality" as sufficiently broad to encompass competition based on privacy offerings or features. Where the law and agency guidance enable antitrust to account for non-price competition more generally, it opens the door to consideration of the quality of data privacy.[191] This retention of the basic consumer welfare premise, even if broadly interpreted, may explain why the privacy-as-quality theory has seen growing acknowledgement and acceptance. It offers a means of accounting for data privacy in a manner that does not require a substantial rethinking of the fundamental tenets of antitrust law.

At the same time, multiple antitrust agencies view the "privacy-as-quality" theory as a jurisdictional limit on their role in addressing privacy concerns. From time to time, privacy advocates and scholars call for antitrust law to be used widely, to protect consumers from data privacy harm untethered to competitive effects. The response of antitrust agencies has been to resist, with reference to the limits of antitrust in considering privacy. For example, Google's acquisition of Doubleclick, an ad serving company, in 2007 raised some concerns that the combination of the merging parties' data sets of consumer information would be used in a way that threatened consumer privacy. In response to these concerns, a majority of the FTC Commissioners found that the agency "lack[s] legal authority to require conditions to this merger that do not relate to antitrust."[192] Similarly, in the 2006 *Asnef/Equifax* merger challenge, the European Court of Justice found that "any possible issues relating to the sensitivity of personal data are not, as such, a matter for competition law, they may be resolved on the basis of the relevant provisions governing data protection."[193] In other words, standalone privacy concerns with no nexus to competition are not considered cognizable in antitrust law.[194] "Pure" privacy harms, unrelated to competition, are viewed by these antitrust authorities and courts as the domain of privacy law and privacy agencies. This is in contrast to privacy-as-quality impacts that

[190] The widely shared goal of modern antitrust law is to improve consumer welfare, through the promotion of competition. This includes competition based not only on price, but also on non-price factors, like quality. *See, e.g.,* Nat'l Soc'y of Prof'l Eng'rs v. United States, 435 U.S. 679, 695 (1978) ("[A]ll elements of a bargain—quality, service, safety, and durability—and not just the immediate cost, are favorably affected by the free opportunity to select among alternative offers.").

[191] Singapore, Data: Engine for Growth *supra* note 14, at ¶ 216 (observing the relationship to non-price guidance).

[192] FTC, *Statement of FTC Concerning Google/DoubleClick*, FTC File No. 071-0170, 2–3 (Dec. 20, 2007), https://www.ftc.gov/system/files/documents/public_statements/418081/071220googledc-commstmt.pdf [*hereinafter* FTC Google/Doubleclick]. See further discussion in Part II. 3. Data Privacy Considerations in Merger Review.

[193] Asnef-Equifax, Servicios de Información sobre Solvencia y Crédito, SL v. Asociación de Usuarios de Servicios Bancarios (Ausbanc), 2006 I-11125, Case C-238/05, at ¶ 56 (June 29, 2006).

[194] Terrell McSweeny, FTC Comm'r, *Big Data: Individual Rights and Smart Enforcement*, Remarks at the European Data Protection Supervisor-BEUC Joint Conference (Sept. 29, 2016).

relate to competition, and which may be taken into account in antitrust analysis.

The major concern with taking a broader view of how privacy relates to antitrust—such as a view that uses antitrust law to police privacy harms unrelated to competition—is that it will dilute and confuse antitrust law doctrine. Such a view would inject privacy concerns, which are often broad, non-economic, and potentially subjective or normative, into antitrust analysis that is otherwise guided by the lodestar of economic consumer welfare, efficiency and competition.[195] Particularly in jurisdictions like the U.S., where antitrust hews most narrowly to a consumer welfare/economic efficiency standard, the worry is that using antitrust to protect privacy will confuse antitrust analysis, disrupting its organizing principle of consumer welfare by blending in non-economic harms and benefits with no clear means of determining which is a priority. This concern is invoked not only in response to calls for antitrust to protect data privacy, but also in a opposition to using antitrust law as a tool to pursue a variety of broader social goals unrelated to economic efficiency, from protecting the environment, to increasing employee wages[196] or protecting small businesses. Like the pursuit of privacy (where it is unrelated to competition), these considerations may be important socio-political goals, but they are viewed as beyond the economic welfare purpose of antitrust law.

a. The Challenges of Analyzing Privacy-Related Quality Effects

Despite the increasing theoretical acceptance that privacy may be an element of competition, the measurement of privacy-related competitive effects is likely to be a challenge in practice. Antitrust analysis at all stages is permeated by price-based tools and methodology. Price effects are a deeply rooted foundation of antitrust law, and the economic models upon which it relies. From market definition and market power analysis, through to measurement of the competitive effects of conduct and mergers, price is the primary touchstone for antitrust analysis and modeling. The measurement of non-price effects has long been recognized as a challenge for antitrust law—privacy quality analysis is simply the latest incarnation of this broader issue.

---

[195] *See, e.g.,* Maureen K. Ohlhausen & Alexander P. Okuliar, *Competition, Consumer Protection, and the Right [Approach] to Privacy*, ANTITRUST L.J. No. 1 (2015) (emphasizing separation between data privacy and antitrust, such that "[s]plicing them together… [to use]… the modern antitrust laws, which are empirically focused on economic efficiency, to remedy harms relating to normative concerns about informational privacy contradicts the specialized nature of these laws and risks distorting them in ways that would leave both the law and consumers worse off."); OECD, Directorate for Financial & Enterprise Affairs Competition Comm., Considering Non-Price Effects in Merger Control, Background Note by the Secretariat, at 30 (June 6, 2018) https://one.oecd.org/document/DAF/COMP(2018)2/en/pdf (citing Ohlhausen and Okuliar).

[196] *See* FTC Google/Doubleclick, *supra* note 192 at 2 (noting the FTC has been "asked before to intervene in transactions for reasons unrelated to antitrust concerns, such as concerns about environmental quality or impact on employees" which are beyond the purpose of antitrust law).

In fact, price-based analysis is so central to antitrust law that arguments continue to be made that antitrust doctrine is inapplicable to markets where consumers do not pay a monetary price for products or services.[197] This includes many of the potential markets and industries where privacy-based competition occurs, such as social media and online search. Where consumers are unable to compare the prices of products, their decisions to adopt a product may instead be driven by quality or other features[198]—features such as data privacy protection. The question of antitrust law applicability to "zero-price" markets is therefore also of relevance to privacy-based competition.[199]

The contention that certain antitrust law concepts cannot be applied in zero-price markets is still being litigated in certain jurisdictions,[200] but several others have firmly rejected this view.[201] The latter jurisdictions, while acknowledging that antitrust doctrine has historically been applied in price-driven markets, tend to view antitrust analysis as sufficiently resilient to adapt to zero-price markets.[202] Germany has gone even further than this, passing legislative amendments to clarify that zero-priced products or services do not preclude the finding of a related antitrust market.[203]

---

[197] OECD, Zero-Price Economy – Annex, *supra* note 22, at 4 (noting that "there may be some limitations to applying competition law to certain types of conduct in zero-price markets in some jurisdictions"); *see, e.g.*, Kinderstart.com, LLC v. Google, Inc., 2007 WL 831806 (N.D. Cal. Mar. 16, 2007) (finding that online search is not a "market" for the purposes of antitrust law, as it is provided for free to end users).

[198] *See, e.g.*, OECD, Directorate for Fin. & Enter. Affairs Competition Comm., Quality Considerations in the Zero-Price Economy - Note by Germany, at 1-2 (Nov. 28, 2018) [*hereinafter* OECD, Zero-Price Economy - Note by Germany] (noting greater importance of qualitative features in driving consumers choices in zero-price markets).

[199] *See* OECD, Zero-Price Markets – Background Note, *supra* note 9, at 36.

[200] Memorandum in Support of Facebook, Inc.'s Motion to Dismiss FTC's Complaint, FTC v. Facebook, Inc. No.: 1:20-cv-03590 (D.D.C Jan. 21, 2021) at 12-13 (challenging the adequacy of a market definition based on cross-elasticity of demand in free services).

[201] *See, e.g.*, Office of Fair Trading (U.K.), Motorola Mobility Holding (Google, Inc.)/Waze Mobile Limited, ME/6167/13, 17 ¶ 8 (Dec. 2013), http://webarchive.nationalarchives.gov.uk/20140402225142/http://www.oft.gov.uk/shared_oft/mergers_ea02/2013/motorola.pdf. (rejecting argument that a zero price renders competition law inapplicable, finding it sufficient that the activities of a business are carried on for the purposes of "gain or reward"); Eur. Comm'n, Google Search (Shopping), Case AT.39740/Decision C (2017) 4444, at ¶ 319-324 (July 27, 2017) (rejecting Google's argument that since search is zero-priced, there could be no market dominance).

[202] *See, e.g.*, Furman Report on Digital Competition, *supra* note 96, at 87 ("Consumer welfare standard analysis can be effective even when monetary prices are zero, as they often are in the digital economy, by considering quality aspects such as privacy, how much better 'free' services might be with more competition, and the possibility that the price might be negative if customers were paid a competitive price for their data.").

[203] *Act Against Restraints of Competition 2013*, as last amended by Article 10 of the Act of 12 July 2018 § 18(2)(a) (Ger.).

However, this growing theoretical acceptance that antitrust law applies to zero price markets still leaves the practical challenge of how to adapt price-focused antitrust analytical tools to evaluate privacy-related effects on competition. Several antitrust agencies acknowledge that the evaluation of quality-based effects on competition is likely to be more difficult than analysis of price-based competition.[204]

The primary difficulty is that there are no settled analytical approaches (or even a clear set of potential alternative approaches) for antitrust to assess changes in the *magnitude* or *quality* of privacy protection in relation to misconduct or mergers. This lack of established, reliable analytical tools to evaluate privacy quality effects is likely to be a significant barrier to the integration of privacy considerations into antitrust analysis. Though early stage, the next section of this Report describes types of evidence that are being used determine whether and how privacy plays a role in competition, and other types of evidence that might be used to understand the specific nature of that competition.

Measuring privacy quality, and the impact on consumers of declining quality, may be difficult for a number of reasons. As privacy literature and agencies have long acknowledged, consumers often have heterogeneous privacy preferences.[205] Some consumers might view additional personal data processing as desirable, if it enables them to use a new service or feature, or to pay nothing for a service. Others might view this as a decrease in quality, and prefer to pay for a service that does not collect their personal information. The former head of the U.S. DOJ Antitrust Division describes this distinction from traditional price-based analysis as the "economic nuance of revealed preference—that is, not every customer values their data, or their privacy, the same way. Money has face value, but privacy cannot yet be measured in nominal terms, and varies according to the type and utility of the data used."[206]

The analysis of privacy quality effects may be further complicated by tradeoffs between privacy and other parameters of quality. Imagine, for example, a digital service that unilaterally changes its terms of service and technology to begin collecting more extensive personal data from its users, without their consent. The additional data collected may be used to improve the relevance

[204] Competition Bureau Canada, Big Data and Innovation: Implications for Competition Policy in Canada, at 23 (2017) https://www.competitionbureau.gc.ca/eic/site/cb-bc.nsf/eng/04304.html (noting some dimensions of quality "may not be directly measurable or may be more difficult to express in dollar terms, such as privacy. Measuring the welfare impacts of non-price effects is challenging"); *Id.* at 9 (observing "the challenges present in analyzing non-price effects"); OECD, Zero-Price Economy - Note by Germany, *supra* note 198, at 4.

[205] OECD, Zero-Price Markets – Background Note, *supra* note 9, at 10 (discussing heterogeneous consumer preference for the exchange of data for services).

[206] Makan Delrahim, Asst. Att'y Gen., Antitrust Div., U.S. Dep't of Justice, Don't Stop Believin': Antitrust Enforcement in the Digital Era (Apr.19, 2018).

of advertising to users or to deliver useful features within the service, like location-based alerts. The competitive effects assessment is made more complicated by the tradeoff between the harm to privacy quality and the improvement in (other) product quality. The change along more than one parameter of quality—improved features but reduced data privacy—makes it more difficult to objectively conclude that the overall product quality has declined.[207]

Finally, privacy quality measurement may be rendered more difficult by the well-documented demand-side distortions among consumers regarding privacy choice.[208] As a result of cognitive biases, information asymmetry and limited or complex choice, consumers may be unable or unwilling to switch away from a product or service, even when privacy quality is eroded to below what the consumer would prefer. Analysis of market definition or competitive effects may need to account for consumer behavioral biases,[209] complicating the measurement of privacy quality harms and effects.

These quality measurement challenges have the potential to permeate antitrust analysis wherever the evaluation of privacy-based competition plays a role, from market definition and market power analysis to the evaluation of anticompetitive effects from conduct or a merger. As the OECD observes, many of the analytical tools developed for market definition and assessment of competitive effects were created to measure price impacts, and therefore "[a]lternative tools are needed to assess demand (and supply) substitutability in respect of quality."[210] The OECD suggests that, in zero-price markets, indicators "such as measures of online user attention, volume of transactions, and assessment of network effects and the prevalence of multi-homing" may be useful in assessing competition.[211]

Another potential approach to analyzing privacy effects is to estimate the monetary value of the data being provided by consumers. Under this conception, consumers "pay" for services with their data, and the antitrust analysis seeks to quantify the value of the collection, use or other processing of that data in price-based terms. For zero-priced services and markets, this approach

[207] Geoffrey A. Manne & R. Ben Sperry, *The Problems and Perils of Bootstrapping Privacy and Data into an Antitrust Framework*, CPI ANTITRUST CHRONICLE 1, 3-5 (May 2015). It may also be that there is no "tradeoff" at all—that more data is simply collected and used to the benefit of the company, while delivering to consumers only the same value as before the change. In such a case, the decline in quality seems more apparent.

[208] See Part I.4.c. Consumer Choice and the Challenge of Demand-Side Distortions..

[209] Crémer Report, *supra* note 110, at 50 (calling for competition analysis in digital markets to account for consumer biases).

[210] *See, e.g.*, OECD, Zero-Price Economy – Annex, *supra* note 22, at 4 (referencing quality trade-offs and heterogeneous consumer preferences).

[211] *Id.*

shoehorns non-price analysis into antitrust price-based models. For other digital products and services, though, the existing business models may provide insight into the monetary value that consumers place on their data or privacy—such as where consumers pay an additional fee to add privacy-protective features to a service, or pay for the version of a service without behavioral advertising, where a free, ad-based version is also offered.

There has been some skepticism expressed over antitrust analysis that translates data privacy or processing into monetary terms (where the market does not already do so),[212] and certain jurisdictions have rejected this approach outright.[213] Though equating data processing to a monetary value may seem convenient for antitrust purposes, it could prove problematic in jurisdictions where data privacy is conceived of as a fundamental right. The former head of the EDPS criticized a proposed digital content directive that treated personal data "in practice . . . as a sort of digital currency."[214] While conceding that personal data has value, he observed that the dignitary nature of privacy rights means that "even if some people treat personal data as commodity, under EU law it cannot be a commodity. . . . You cannot monetise and subject a fundamental right to a simple commercial transaction, even if it is the individual concerned by the data who is a party to the transaction."[215]

However, in jurisdictions like the U.S. where data privacy is a consumer protection interest rather than a fundamental right (at least at the federal level), equating data or privacy impacts to monetary terms will not raise such deeply rooted incompatibilities. At the same time, this analytical approach may not necessarily overcome the difficulties discussed above in measuring privacy effects. The determination of the monetary value consumers place on privacy or data processing is still likely to face challenges in how to account for consumer biases, and the tradeoffs between data disclosure and other facets of product or service quality. The OECD concludes that, instead of equating data to currency, analysis akin to that of "any other dimension of quality remains the most practical approach."[216]

[212] OECD, Zero-Price Markets – Background Note, *supra* note 7, at 15; Delrahim, Don't Stop Believin', *supra* note 206 (expressing skepticism over antitrust analysis that "simply *declare*[s] that data is the new digital currency").

[213] OECD, Zero-Price Economy - Note by Germany, *supra* note 198, at 3 (rejecting the equation of data to "currency" in analyzing multi-sided zero-price markets in light of what is often a price-based (other) side of the platform).

[214] Giovanni Buttarelli, Address to Socialists and Democrats Group Workshop on the Proposed Digital Content Directive, Eur. Parliament (Jan. 12, 2017).

[215] *Id.*

[216] OECD, Zero-Price Markets – Background Note, *supra* note 9, at 15.

Overall, the approaches to measuring effects on privacy from competition are at a nascent stage, but play a central role in the integration of privacy consideration into many aspects of antitrust analysis. A 2018 OECD report on zero-price markets observes that there have been few novel approaches introduced to quantify quality-based effects in such markets—which would include privacy effects—since the issue was last examined 5 years prior.[217] The OECD concludes that "the degree to which [privacy] is quantifiable is limited by the lack of meaningful measures from a consumer and competition perspective."[218]

As these comments imply, there is a significant opportunity for collaboration between data privacy and antitrust authorities to develop reliable, well-founded methodology and tools to measure competition-related effects on privacy quality. In particular, the expertise of data privacy authorities regarding the measurement and evaluation of privacy, and the effects of market conduct on privacy levels could provide valuable insight to antitrust authorities who are seeking to evaluate privacy-based effects on competition.

i. Early Approaches: Measuring Privacy-Based Competition

Despite the likely analytical challenges in measuring privacy effects, antitrust law has some early-stage approaches to this task that are worth mentioning. At a more general level, these sources of evidence are familiar to antitrust analysis—survey evidence, market behavior evidence and internal documents—but their adaptation to understand privacy-based competition is new.

There are few publicly available examples, with little detail and no settled methodology or best practices yet apparent across jurisdictions. However, the following types of evidence have been discussed or used in antitrust analysis as a means to determine whether there is privacy-based competition, and its parameters:

- **Survey evidence on whether data privacy is a driver of competition:** Antitrust authorities often survey the consumers or businesses likely to be impacted by conduct or mergers, to understand the market and the likely effects on competition. Antitrust authorities could similarly gather survey data about whether and how privacy is viewed as a parameter of competition in a given market. Consumer survey evidence may need to be interpreted with an eye to the demand-side distortions described above, such as the

[217] *Id.*

[218] *Id.*

widely recognized differences between stated and revealed privacy preferences.[219] However, competition authorities also regularly rely on surveys of market participants (other businesses) to inform their views in merger and conduct cases. The European Commission used such questionnaires as part of its evaluation of the Microsoft/LinkedIn merger in 2016, including to inform its understanding of the role privacy plays in competition between professional social networking services.[220] The case, and the findings of privacy-related competitive effects, are described depth below.[221]

- **Observation of market behavior:** Where privacy policies or other behaviors have changed in the relevant market, the responses of consumers and rivals to that change may inform the analysis of whether privacy is an important parameter of competition. For example, if one competitor modifies their privacy policy to increase (or decrease) an aspect of data privacy protection, such as the length of time data is retained, do other competitors then follow suit? If so, that may suggest there is competition related to privacy policy terms in the market. The content, length and readability of privacy policies may also provide insight into privacy-based competition, as companies seek to convey their privacy practices to consumers.

- **Internal documents of merging parties or firm(s) in conduct cases:** In antitrust investigations and cases the internal documents of companies have long been an important source of evidence, particularly where the documents pre-date the initiation of the antitrust action. Specifically, internal documents may provide insight into the rationale for changes to privacy policies. The OECD describes, for example, the potential for "documents proving that businesses track the privacy policies of other companies" to indicate privacy-based competition.[222] Internal documents could also indicate the parameters of privacy that are seen as relevant to competition by merging parties, or the expected effects on measures of privacy that will arise from conduct or mergers.

  In a recent abuse of dominance case, the Canadian Competition Tribunal was persuaded by the *absence* of contemporaneous documents discussing user privacy.[223] The defendant

[219] OECD, Zero-Price Markets – Background Note, *supra* note 9, at 15-16 (noting that "consumer surveys could be used to gauge the confidence that consumers have in a firm's privacy arrangements, although these perceptions may not match reality").

[220] Eur. Comm'n, *Microsoft/LinkedIn*, Case No. M.8124 C (2016) (June 12, 2016).

[221] *See* Figure 5. Case Study of the European Commission's Review of the Microsoft/LinkedIn Merger.

[222] OECD, Consumer Data Rights and Competition – Background note, *supra* note 9, at 38.

[223] *Comm'r of Competition v. Toronto Real Estate Bd.*, 2016 Comp. Trib. 7 (Can.).

claimed that its anticompetitive conduct was driven by a desire to protect end-users' privacy on its real estate sales platform. The Tribunal found that these claims of user privacy protection were merely pretextual, in part due to the lack of any proffered documentary evidence reflecting the purported concerns over user privacy impacts.[224]

- **Finally, the OECD suggests that competition analysis could be informed by the amount of data processed**, and provides the following examples of potential measurements of data processing: "(1) the scope of data collection, or in other words the number of variables for which data is collected, (2) the frequency of data collection (e.g. only at the point a consumer signs up for an account, or each time a consumer uses the service), (3) whether data collection is limited to a consumer's interaction with the service in question, or whether data collection continues while the consumer is using other services, and (4) the degree to which this data is shared with other parties, including other business units within the firm, and externally, through data brokers for example."[225] However, the OECD notes that, to be informative as a measure of privacy, "the volume of data collected must be put in context of how it is processed and treated by firms, as well the firm's data security safeguards."[226]

The first three types of evidence listed above may be helpful in determining the role privacy in competition within a specific market. However, quantification of the magnitude of privacy-based effects (rather than the mere existence of privacy competition) is likely to continue to be a challenge, for the reasons described in the prior section of this Report.

2. Market Power, Market Definition and the Challenge of Zero-Price Markets for Antitrust Law

The starting point for antitrust analysis is often the definition of the relevant antitrust markets, and an assessment of whether the firm being scrutinized holds market power. Market power is "the ability to raise prices above those that would be charged in a competitive market,"[227] or the

[224] *Id.* See further discussion of this case in Figure 7. Case Study: User Data Privacy as a Justification for Anticompetitive Conduct— The Canadian Competition Tribunal and the Toronto Real Estate Board.

[225] OECD, Zero-Price Markets – Background Note, *supra* note 9, at 16.

[226] *Id.*

[227] NCAA v. Bd. of Regents of the Univ. of Okla., 468 U.S. 85, 109 n.38 (1984).

similar ability to lower quality or output below that which would exist in a competitive market, while still maintaining profitable sales levels.[228]

While acknowledging that digital markets may pose specific analytical challenges, antitrust agencies have tended to reaffirm the resiliency, flexibility and applicability of existing analytical frameworks for market power and market definition.[229] Market power analysis in digital markets, as in traditional markets, has therefore sought to define the relevant market and evaluate market shares, closeness of competitors, competitive constraints, barriers to entry and expansion, actual new entry/exit and any scope or scale advantages. Within these existing frameworks, though, antitrust enforcers recognize that digital markets often exhibit specific features that impact and add complexity to antitrust analysis, such as prevalent network effects and the heightened importance of non-price competition.[230]

Neither market definition nor market power analysis have focused expressly on privacy. Instead, antitrust authorities have looked at the broader considerations posed by digital markets, including the challenges of zero-price products and the role of data in competition. These broader topics are discussed here as issues that may dovetail with the interests of privacy enforcers. Since price cannot form the basis for competition in zero-price markets, privacy and other aspects of product quality may take on a more prominent role in competition in these same markets.

a. Market Definition and Privacy Quality

The definition of the relevant antitrust market is often an important step in evaluating market power and anticompetitive effects in mergers and abuse cases.[231] This analysis seeks to

[228] *See, e.g.*, U.K. Competition Commission, Guidelines for Market Investigations: Their Role, Procedures, Assessment and Remedies (April 2013) at 7 (describing market power "the ability to maintain prices above the competitive level, or restrict output or quality below competitive levels, without the consequent loss of sales becoming unprofitable"). The Competition Commission has since become the U.K. Competition and Market Authority.

[229] *See, e.g.*, Competition Bureau Canada Big Data Report *supra* note 68, at 6 ("in assessing mergers and monopolistic practices [involving big data], the Bureau will generally apply its traditional analysis of market definition, market power, and competitive effects"); ACCC Digital Platforms Inquiry Final Report, *supra* note 117, at 65 (applying traditional concepts of antitrust analysis to evaluate market power of Google); OECD, Zero-Price Economy-Note by Germany, *supra* note 198, at 2 (observing zero-price markets have long existed outside of the digital economy and have been analyzed in the past by antitrust authorities, but are now becoming more prevalent, and may pose some new challenges to antitrust analysis).

[230] OECD, Zero-Price Economy - Note by Germany, *supra* note 198, at 2.

[231] Walker Process Equip., Inc. v. Food Mach. & Chem. Corp., 382 U.S. 172, 177 (1965) ("Without a definition of that market there is no way to measure [a defendant's] ability to lessen or destroy competition."); but *see also* Crémer Report, *supra* note 110, at 3 (noting some jurisdictions have somewhat de-emphasized market definition in antitrust analysis).

determine the relevant group of products and the geographic area where competition takes place. Market definition analysis tends to center on buyers' views about which products (or locations) are reasonably substitutable for the same purpose, based on considerations such as price, quality and intended use.[232]

A common analytical tool used to assess substitutability and define markets, particularly in modern merger review, is the hypothetical monopolist paradigm.[233] This analysis considers a fictional monopolist who imposes a small but significant non-transitory increase in price or "SSNIP" of its products or services, while keeping other parameters are kept constant. The market is defined as comprising the group of products (or services) over which the monopolist could profitably impose a SSNIP, rather than losing profits from sales diverted to the next-best substitute.

For the purposes of the discussion here, the important point is that the hypothetical monopolist test relies on changes in price alone. This approach is ill-fitting for zero-price markets, where consumers pay no monetary fee for the product or service, and non-price factors drive their product choice. There is often no price on which to base the measurement of such effects, at least for the end consumer-facing side of the business.

For products or services in zero-price markets, multiple jurisdictions have posited that, instead of focusing on the effects of a price increase, antitrust analysis might use a small but significant non-transitory decrease in *quality* (SSNDQ) test to define relevant markets.[234] Where a monopolist could reduce a parameter of product quality in a small but significant non-transitory way, without losing users, those products would be considered to be in the same antitrust market.

[232] *See, e.g.,* United States v. E. I. du Pont de Nemours & Co., 351 U.S. 377, 404 (1956) (the antitrust "market is composed of products that have reasonable interchangeability for the purposes for which they are produced—price, use and qualities considered."). Courts will also consider "practical indicia" such as industry or public recognition of a product's unusual characteristics or uses. *See, e.g., Brown Shoe Co. v. United States*, 370 U.S. 294 (1962).

[233] *See* U.S. Dep't of Justice & Fed. Trade Comm'n, Horizontal Merger Guidelines (2010) §4.1.1 (discussing the hypothetical monopolist test). Note that there are recognized limitations in using the hypothetical monopolist test in cases of abuse of dominance, as opposed to merger review, because prevailing prices may already be affected by the dominant firm's exercise of monopoly power. However, there is also no widely accepted alternative for market definition in abuse cases.

[234] Rod Sims, ACCC, *Gilbert and Tobin Seminar: The Data Economy* (Oct. 15, 2018), https://www.accc.gov.au/speech/gilbert-tobin-seminar-the-data-economy (describing the potential use of a SSNIP test modified to measure a degradation in quality of service instead of price); Competition Comm'n Singapore in Collaboration with Intellectual Prop. Office of Singapore and PDPC, *Data: Engine for Growth*, *supra* note 34, at n. 167 (observing that SSNIQ (quality) test "may be used in industries where quality measures are well-accepted and quantifiable"); *see also* OECD, Zero-Price Markets – Background Note, *supra* note 9, at 14.

The research for this Report found no instances where this analytical approach had been used to define markets based specifically on privacy protection or quality, nor has there been any clear need to do so. However, if privacy is considered a material element of quality-based competition among the products or services being analyzed, then, in theory, an SSNDQ test might be used to assess whether monopolists are able to profitably impose a decline in privacy quality.

Discussion of the SSNDQ analysis tends to acknowledge that it will be more difficult to operationalize such a quality-based test than it is the standard, price-based approach.[235] Precise measurement of effects on privacy quality may be challenging for the reasons discussed above, such as heterogeneity in consumer privacy preferences, and tradeoffs between privacy and other product features. The definition of markets may need to account for insights from behavioral economics about consumer biases toward default options and present gratification.[236] These phenomena may all make it more difficult to precisely measure quality effects.

This analysis is further complicated by the two-sided nature of many digital markets, where one group (often the end consumers) receives the products free of charge, while another group pays a monetary price that subsidizes the non-paying side. An example is online search advertising, where end consumers pay no monetary price to use a search engine, but advertisers bid to purchase ads, which the search engines displays to consumers using the search services. The Crémer Report on European competition policy observes that cross-side effects in such markets can add complexity to the valuation of changes in service quality.[237] It concludes that, given the challenges of applying an SSNDQ analysis in zero-price markets, "[the] idea is therefore probably more useful as a loose conceptual guide than as a precise tool that courts and competition authorities should actually attempt to apply."[238]

Another approach to market definition is to simply focus on the substitutability of the function provided by a service or product in a market, without resorting to quality-change modeling.[239] For example, if a given social network application is used to connect and build a professional network, other apps that provide substitutable functionality would be considered within the same market. This approach has been the subject of some criticism for its lack of analytical rigor

[235] Crémer Report, *supra* note 110, at 45; Sims, *supra* note 234 (acknowledging that "determining the impact of a significant deterioration in quality may be more difficult than calculating the impact of a SSNIP").

[236] Crémer Report, *supra* note 110, at 50.

[237] *Id.* at 43.

[238] *Id.* at 45 (quoting the OECD, without a specific source attribution).

[239] *See, e.g., id.;* United States v. E. I. du Pont de Nemours & Co., 351 U.S. 377, 404 (1956) (defining markets "composed of products that have reasonable interchangeability for the purposes for which they are produced—price, use and qualities considered").

relative to the SSNIP test.[240] However, given the perceived challenges in conducting a precise SSNDQ analysis, the Crémer Report suggests such demand substitutability analysis serves a useful role in market definition.[241] After all, as mentioned at the outset of this section, this concept of demand substitution is at the core of most approaches to market definition.

Finally, privacy authorities have suggested that antitrust analysis on substitutability could also reveal insights relevant to data privacy law.[242] Where the competition analysis finds that a service or product is *not* substitutable, the EDPS has suggested this conclusion could inform data privacy determinations of whether the purpose limitation principle is met.[243] Where a service is found non-substitutable, data processing for the purpose of that same service may also be viewed as incompatible with the purpose for which the data was originally collected.[244]

b. Market Power: The Role of Data and Network Effects

The relationship between privacy and market power is not yet well-understood.[245] Antitrust authorities have paid more extensive recent attention to whether and when data might confer market power or a competitive advantage,[246] rather than questions specific to personal data or privacy. The themes from those antitrust agency discussions are described here. An important caveat to this general discussion is that market power is evaluated on a case-by-case basis in antitrust law. The analysis will depend on careful, contextual attention to the specific type of data and its role in competition in the particular market at issue.

[240] Crémer Report, *supra* note 110, at 45-46.

[241] *Id.*

[242] Preliminary Opinion of the EDPS, Privacy and Competitiveness in the Age of Big Data: the Interplay between Data Protection, Competition Law and Consumer Protection in the Digital Economy 27 (Mar. 2014) (suggesting shared relevance of substitutability in competition and purpose limitation analysis in data privacy law).

[243] *Id.*

[244] *Id.*

[245] *See also* Part II.4.a. The Relationship Between Monopoly, Competition and Data Privacy.

[246] *See, e.g.,* Singapore, Data: Engine for Growth *supra* note 14; Competition Bureau Canada Big Data Report *supra* note 68; EDPS, Preliminary Op. of the EDPS, Privacy and Competitiveness in the Age of Big Data (March 2014); Fed. Cartel Office (Bundeskartellamt) (Ger.) & The Competition Auth. (Autorité de la Concurrence) (Fr.), Competition Law and Data (May 10, 2016), https://www.bundeskartellamt.de/SharedDocs/Publikation/DE/Berichte/Big%20Data%20Papier.pdf?__blob=publicationFile&v=2.

Multiple reports on the digital economy in the antitrust context have considered whether the scale and scope of data accumulation may act as a barrier to competition.[247] First, antitrust agencies have considered the potential for data accumulation, and data use, to create barriers to entry and expansion to enhance market power. This often includes consideration of whether the data set that provides a perceived competitive advantage is replicable by competitors,[248] and analysis of data-driven economies of scale and scope.[249] Where a firm accumulates data that is unique and difficult for competitors to replicate in scale or type, that data may create challenges for competitive entry and contribute to market power.[250] For example, the French and German competition authorities issued a joint report on competition and data, which explains that the "collection of data may result in entry barriers when new entrants are unable either to collect the data or to buy access to the same kind of data, in terms of volume and/or variety, as established companies."[251] The Singapore competition authority has proposed changes to its agency guidance to clarify that data may constitute a barrier to entry in a market.[252]

[247] Crémer Report, *supra* note 110, at 99-100 ("The prominent position of data in digital markets may make it difficult for new entrants to compete on the market without access to a significant pool of data. . . . In some settings, we can expect the foreclosure effects from a refusal to grant access to data to be high, in particular if a high degree of market concentration translates into a high degree of data concentration, and if that data yields an important competitive advantage in serving neighbouring markets. In such a setting, the need to ensure the possibility of entry may argue in favour of mandating access to data."); Furman Report on Digital Competition, *supra* note 96, at 9 (identifying "the central importance of data as a driver of concentration and barrier to competition in digital markets" as a key theme of the evidence gathered by the review of digital markets).

[248] *See, e.g.*, Competition Comm'n of Singapore, Intellectual Prop. Office of Singapore & Personal Data Protection Comm'n, *Data: Engine for Growth – Implications for Competition Law, Personal Data Protection, and Intellectual Prop. Rights* (Aug. 16, 2017) (considering whether data could be replicated reasonably by competitors, and whether the data could result in a significant competitive advantage).

[249] Crémer Report, supra note 110, at 2-3 (observing relevance of network effects in digital economy; noting economies of scale appear in many industries, but that "the digital world pushes it to the extreme and this can result in a significant competitive advantage for incumbents."); ACCC Digital Platforms Inquiry Final Report 2019, *supra* note 71, at 73 (same).

[250] *See, e.g.*, ACCC Digital Platforms Inquiry Final Report, *supra* note 71, at 68 (finding barriers created by Google's accumulation of data, and concluding that "such data can be expected to provide Google with a substantial comparative advantage, on account of the considerable magnitude of Google's search data relative to its rivals, both in Australia and globally.").

[251] Fed. Cartel Office (Bundeskartellamt) (Ger.) and The Competition Auth. (Autorité de la Concurrence) (Fr.), Competition Law and Data (May 10, 2016), https://www.bundeskartellamt.de/SharedDocs/Publikation/DE/Berichte/Big%20Data%20Papier.pdf?__blob=publicationFile&v=2.

[252] *See, e.g.*, Competition & Consumer Comm'n of Singapore, *Proposed Amendments To The* CCS *Guidelines*, *Consultation Document*, at Annex D (Sep. 10, 2020), https://www.cccs.gov.sg/public-register-and-consultation/public-consultation-items/2020-public-consultation-on-proposed-changes-to-competition-guidelines (proposal to update merger guidance that "data" may constitute a barrier to entry or expansion).

Second, there has also been some agency attention to the possibility of data-driven feedback loops, wherein incumbents with superior access to data are, in turn, better able to improve and refine their data-driven products.[253] Such feedback may represent competition on the merits, where data collection is used to improve products or services in a manner that benefits consumers. However, there has also been some concern that such effects could make new entry and expansion more difficult for those without a similar data-driven advantage.[254]

Third, much attention has been paid to the features of digital markets that may amplify—or in some cases reduce—data-driven effects on market power. In particular, there has been a significant focus on the role of network effects in influencing market power.[255] Network effects occur in many types of digital services, such as social networking or sharing ("gig") economy services, where the larger the number of users, the more valuable the service becomes to other users. Network effects tend to be described as bolstering the market power of incumbent firms. They may act as a barrier to entry, raising switching costs for users who would otherwise change networks, and rendering markets prone to tipping toward a single, large provider. For example, in a 2019 report, the ACCC considered the impact of network effects in the evolution of Google's market power over time in online search and search advertising. It found that cross-side network effects could operate as a barrier to entry and expansion in general search services.[256] It also found cross-side network effects—the more users Google attracts to its search services, the more data it has, which improves its competitive advantage in attracting and supplying advertisers on the "other side" of its search platform.[257]

However, antitrust agencies have also recognized that network effects may amplify the competitive viability of a new entrant to a market. The German Competition authority reached this conclusion in the Immonet/Immowelt merger, discussed in **Figure 4. Case Study on the Immonet/Immowelt German Competition Authority Merger Clearance Decision**, below.

[253] Furman Report on Digital Competition, *supra* note 96, at 33 (discussing data feedback loops and data as a barrier to entry); CMA Online Platforms and Digital Advertising Market Study, *supra* note 94, at Appendix I (finding that Google has a self-reinforcing data advantage in search, where it receives more data, which drives more relevant search results, subsequent demand and further data).

[254] Furman Report, *id.*

[255] OECD, Zero-Price Economy - Note by Germany, *supra* note 198, at 3-5; Competition Bureau Canada Big Data Report, *supra* note 68 (noting cross-side effects of platforms and network effects as frequently important in analyzing data-driven markets); ACCC Digital Platforms Inquiry Final Report, *supra* note 71, at 67 (evaluating cross-side network effects); Singapore, Data: Engine for Growth, *supra* note 14 (noting market power would generally be strengthened by network effects but could be weakened by multi-homing, ease of access and data substitutability).

[256] ACCC Digital Platforms Inquiry Final Report *supra* note 71, at 67.

[257] *Id.*

Figure 4. Case Study on the Immonet/Immowelt German Competition Authority Merger Clearance Decision

Network effects are typically described as creating barriers to competitive entry or expansion. However, in the Immonet/Immowelt transaction, network effects and multi-homing played a positive role in the German competition authority's decision to clear the merger. The German competition authority (Bundeskartellamt) approved this merger between the second and third largest online real estate platforms in Germany, on the basis that the transaction could prevent the market from tipping to a monopoly held by the market-leading firm.

The online real estate platforms acted as intermediaries between real estate sellers and buyers. Buyers paid nothing while sellers paid fees. There were positive cross-side network effects in the market, meaning that as more real estate sellers joined the platform, more buyers were attracted to it and vice versa. The German competition authority concluded that the merger "provided the opportunity for a second big platform to promote multi-homing by service users, thus intensifying competition."[258] The decision illustrates that the impact of network effects is context-dependent, and that such effects may play a positive role in enabling greater competition against an incumbent.

Finally, market shares continue to play a highly influential role in evaluations of market power.[259] Where a firm is found to have a high market share in a relevant antitrust market, this is not sufficient to conclude that it has market power, but it often contributes significantly to this conclusion.

In some zero-price markets, the measures of market share may be distinct from those in price-driven markets, where revenue or profit shares are often used. For example, the OECD suggests that zero-price markets may measure share based on users, or share of relevant interactions (such as views, searches or transactions).[260] Such measures may be impacted by multi-homing—when

[258] OECD, Zero-Price Economy - Note by Germany, *supra* note 198, at 6; Case Summary, Immonet/Immowelt, decision of 20 April 2015, B6-39/15.

[259] *See, e.g.*, ACCC Digital Platforms Inquiry Final Report, *supra* note 71, at 65, Fig. 2.2 (noting Google's high market share of general search services in Australia); Complaint, U.S. Dept. of Justice v. Google, No. 1:20-cv-03010 (D.D.C. Oct, 20, 2020).

[260] OECD, Zero-Price Markets – Background Note, supra note 9, at 15; *see, e.g.*, ACCC Digital Platforms Inquiry Final Report, *supra* note 71, at 65, Fig. 2.2 (noting Google's high market share of general search services in Australia, by page views); Eur. Comm'n, Decision C (2017) 4444, Case AT.39740 – Google Search (Shopping) (July 27, 2017), http://ec.europa.eu/competition/antitrust/cases/dec_docs/39740/39740_14996_3.pdf (noting Google's stable market share by volume).

individual consumers use multiple products for the same purpose.[261] Ultimately, the appropriate market share measure will be highly specific to the antitrust market and parties, and is often the subject of debate.

c. Conclusions on Market Definition and Market Power Analysis in Practice

Though there are theoretical challenges for antitrust law in the definition of zero-price markets and measurement of market share in digital contexts, in practice, those issues have not stymied antitrust enforcement. Antitrust agencies have defined digital markets in relation to the services offered by several large digital platforms, despite those services being zero-priced for end consumers. Multiple antitrust agencies have concluded that specific digital companies possess market power, often emphasizing the persistence of high market shares over time. For example, in its 2019 Digital Market Inquiry Final Report, the Australian competition authority found that Google and Facebook have market power in Australia in the supply of general search services and social media, respectively, and that the companies' high market shares have persisted for many years.[262] Recent U.S. monopolization cases against Facebook and Google similarly allege that the companies hold market power in the U.S.[263] Although these conclusions have not yet been tested in litigation, the overall impression is that the theoretical challenges in market definition are not so significant, or perhaps not so central to the analysis of market definition or market power, as to create insurmountable case-by-case issues.

The research for this Report suggests data privacy has not played much, if any, role in the analysis of market definition or market power. If privacy does become more important in such analysis for a particular case, the expertise of data privacy authorities in measuring and evaluating data privacy will be valuable in informing the antitrust analysis.

3. Data Privacy Considerations in Merger Review

This section considers the role of data privacy in the review of mergers by antitrust authorities. Merger review is one of the more developed touchpoints between antitrust and data privacy, both in theory and practice. Although still new, it has a slightly longer history, more decided cases, and it has received greater attention from agencies than other topics at this intersection.

---

[261] OECD, Zero-Price Markets – Background Note, *supra* note 9, at 15.

[262] ACCC Digital Platforms Inquiry Final Report, *supra* note 71, at 65, Fig. 2.2 (noting Google's persistently high market share of between 93-95% of general search services in Australia, by page views, from 2009 to 2018)

[263] Complaint at ¶¶ 52-57, U.S. Dept. of Justice v. Google, No. 1:20-cv-03010 (D.D.C. Oct, 20, 2020); Complaint, FTC v. Facebook, Inc. No.: 1:20-cv-03590 (D.D.C Jan. 21, 2021).

However, this assessment is relative—the role of data privacy in merger reviews is still very much at an early stage of theory and understanding.

Competition agencies around the world are empowered to review and challenge mergers and other corporate transactions that are likely to cause significant, negative effects on competition.[264] Though the specific laws vary, an estimated 135 jurisdictions have some form of a merger review regime.[265] Many of those laws also require the merging parties to file an advance notification of their transaction with antitrust agencies for those mergers that meet certain financial thresholds for party and/or deal size.

As early as 2006-2007, antitrust authorities began to contemplate the potential relevance of privacy-based competition in their review of mergers.[266] The agency perspective has tended to be that of the privacy-as-quality paradigm described above: is the merger likely to impact privacy as an element of quality-based competition in the relevant market(s)?[267] Consumers may prefer one product over another based on the competitiveness of the different privacy attributes offered by each product. Where the merging parties' products compete based on privacy features, antitrust agencies will consider the effects of the merger on such privacy-based competition. If the proposed merger would reduce privacy-based competition in a relevant market, that impact will be considered within the overall antitrust analysis of whether the merger is likely to substantially reduce competition.

Privacy quality reductions as a result of a merger might include, for example, i) a degradation in the level of privacy protection afforded, or ii) an increase in personal data processing without offsetting product/service benefits. This could include slower or less accurate services, despite the collection and use of the same amount of personal data by the entity offering those services. Or, it could involve an increase in the amount of behavioral advertising, with no offsetting benefits for consumers. The analysis of any effects from a merger must be fact-driven and specific to the transaction. The relevance of privacy arises from the consideration of how competition occurs or is affected on the facts in a given market.

[264] Although the term "merger" is used throughout this section for simplicity, it is possible that other types of non-merger competitor collaborations, such as joint ventures, could raise similar analytical issues for antitrust agencies. *See, e.g.*, Figure 8. Case Study: Colombia Digital Identity Joint Venture (discussing remedies recommendations that focus on interoperability and privacy for a joint venture between Colombia's three largest banks).

[265] OECD, Global Merger Control: OECD Competition Trends, Volume II 2021, at 7 (noting as of 2019, 135 jurisdictions around the world have merger laws or regulations).

[266] FTC Google/DoubleClick, *supra* note 192, at 2-3.

[267] *See* Part II.1. Integrating Data Privacy into Antitrust Analysis: The "Privacy-as-Quality" Theory.

The U.S.[268] and European[269] competition authorities have now considered privacy as a potential parameter of quality-based competition in multiple mergers, which are discussed throughout this Report section. Antitrust authorities in several other jurisdictions describe a theoretical acceptance of the view that privacy could be a parameter of competition in certain markets.[270] For example, Singapore has proposed amendments to its merger guidance to clarify that competition authority may consider effects on data privacy where it is a significant parameter of competition, or harmed by quality-related rivalry.[271]

Despite growing theoretical acceptance of this privacy-as-quality paradigm, it has proven relevant on the facts in only a small number of merger reviews. Even on those occasions where privacy-based competition is considered, agencies have rarely found that privacy-related effects on competition arises as a result of a merger.[272] For example, in its review of the *Facebook/WhatsApp* merger, the European Commission considered whether privacy was a relevant parameter of competition in the market for "consumer communications apps."[273] The

[268] FTC Google/DoubleClick, *supra* note 192.

[269] *See, e.g.*, Eur. Comm'n, Facebook/WhatsApp, Case No. COMP/M.7217 C(2014) 7239, ¶ 174 (Oct. 3, 2014) (acknowledging privacy as a non-price element of competition); Eur. Comm'n Press Release IP/16/4284, Mergers: Commission Approves Acquisition of LinkedIn by Microsoft, Subject to Conditions (Dec. 6, 2016), https://ec.europa.eu/commission/presscorner/detail/en/IP_16_4284 (same); Eur. Comm'n Press Release IP/20/2484, Mergers: Commission Clears Acquisition of Fitbit by Google, subject to Conditions (Dec. 17, 2020).

[270] Competition Bureau Canada Big Data Report *supra* note 68 ("It is conceivable, for example, that in some cases consumers may view privacy as an important element of quality. The Bureau is aware of no convincing evidence to rule out categorically privacy as a factor that may affect consumer perception of the quality of a service that uses big data, and as a result could be a relevant dimension of competition between firms."); Singapore, Data: Engine for Growth *supra* note 14, at 14 (noting "where data protection is a non-price factor of competition, the treatment of personal data may affect how [the competition authority] considers and assesses the competitive dynamics of a market"); Interview by the Off. of the Privacy Comm'r, The Danish Competition and Consumer Authority (Jun. 2020) (noting though it has not yet been an issue in a proposed merger, privacy harms could be considered).

[271] Comp. & Consumer Comm. Singapore, Proposed Amendments to the CCS Guidelines, Consultation Document, Sept. 10 2020 at Annex D, 14 (proposal to update merger guidance to clarify that data protection can be an aspect of competition considered, where relevant, in merger analysis), available at https://www.cccs.gov.sg/-/media/custom/ccs/files/media-and-publications/media-releases/2020-public-consultation-on-proposed-changes-to-competition-guidelines/cccs-guidelines-amendments-2020--media-release-10-sept-2020.pdf?la=en&hash=4C25562ACFF7BC265CA3AB72F89BCA673AF060F0.

[272] *See, e.g.*, OECD, Competition Trends 2021, Volume II, Global Merger Control, at 29 (2021) (noting data protection has been "considered a dimension of quality in a limited number of recent merger decisions"), https://www.oecd.org/daf/competition/oecd-competition-trends-2021-vol2.pdf ; OECD, Zero-Price Markets – Background Note, *supra* note 9, at 7 (noting that "competition on privacy appears to still be observed in only a minority of competition cases. This may stem from decisions on the part of firms not to differentiate themselves in terms of privacy (perhaps due to a lack of competitive pressure to do so), and difficulties for consumers in evaluating privacy quality").

[273] Eur. Comm'n Competition Merger Brief M.8124, *Microsoft/LinkedIn*: Big Data and Conglomerate Effects in Tech Markets 5 (May 2017), https://ec.europa.eu/competition/publications/cmb/2017/kdal17001enn.pdf (describing conclusion in *Facebook/WhatsApp* that privacy was not a major basis for competition).

agency found that privacy was not a strong basis for competition and "was only one of many parameters driving user choice" of such apps.[274] The Commission concluded that the *Facebook/WhatsApp* merger would not lead to consumer harm from potential degradation of privacy-based competition.[275]

The European Commission's review of the *Microsoft/LinkedIn* acquisition is one of the few mergers in which privacy-related competition effects have been found likely to occur.[276] LinkedIn offers a popular professional social networking service. The Commission concluded that, as a result of its acquisition of LinkedIn, software giant Microsoft would have the incentive and ability to use its strong market position to exclude competing providers of professional social networking, with likely detrimental effects on the privacy options available to consumers. First, Microsoft would be able to integrate LinkedIn features into Microsoft's widely-used Office software suite, and deny rival social networking services similar access. Second, Microsoft could require that personal computer (PC) manufacturers pre-install LinkedIn as the default social networking service on PCs running Windows, Microsoft's popular operating system. The Commission found that such conduct was likely to marginalize rival professional service networks from competition. Since some of these competing social networks offered greater privacy protection, the merger was likely to reduce consumer privacy options in the relevant market. In response to these concerns, the Commission imposed various obligations on the parties as a condition of merger approval, all targeted at maintaining post-merger competition. The *Microsoft/LinkedIn* case is discussed in more depth in **Figure 5. Case Study of the European Commission's Review of the Microsoft/LinkedIn Merger**, below.

The privacy foreclosure finding in *Microsoft/LinkedIn* makes it one of few mergers in which privacy-related effects on competition were actually found to be likely, rather than simply considered and dismissed. The case is also notable because, although the parties did not compete with each other pre-merger to provide privacy protection in social networking services, the transaction was still found likely to erode privacy competition. Such effects on competition are termed "conglomerate effects"—where the parties involved are not actual or potential competitors at the time of merger, but they have complementary products such that the merger leads to an increased ability to exclude rivals from a relevant market.

[274] *Id.*

[275] *Id.* at 1.

[276] *Id.*

Figure 5. Case Study: The European Commission's Review of the *Microsoft/LinkedIn* Merger

In 2016, Microsoft, a leading personal computer software company, sought to acquire LinkedIn, which operates one of the most popular professional social media platforms. As part of its review of the merger, the European Commission expressed concerned that the transaction would enable Microsoft to leverage its strong market position in personal computers and software to foreclose competing professional social networks.

At the time of the transaction, Microsoft Windows was installed on 80-90% of new personal computers within the EU. The Commission was concerned that Microsoft would have the ability and incentive to require personal computer manufacturers to pre-install LinkedIn as part of the Microsoft Windows operating system. Microsoft could demand exclusivity to prevent manufacturers from installing competing social media software. Even if exclusivity was not required, there would be little practical incentive to install competing social network software that duplicated LinkedIn's functionality. Further, the Commission found that Microsoft, as a leading supplier of workplace software, could integrate LinkedIn into its popular Microsoft Office applications, then deny competing professional social networks similar access.

The Commission found that the anticipated integration of LinkedIn into Microsoft products, and default featuring of LinkedIn on those products were likely to marginalize competing professional service networks. This risk was exacerbated by network effects that characterized the relevant market, which increased the potential for the market to "tip" toward a single, large social networking service.

The Commission noted that, relative to LinkedIn, a social network rival called XING offered stronger privacy protection in its policies, terms and consent to policy changes. The agency found that if Microsoft foreclosed competition from such rival social networking companies, which offered greater privacy protection than LinkedIn, the transaction would likely reduce the available consumer privacy options. Although this privacy conclusion was just part of the Commission's broader analysis of the transaction, *Microsoft/LinkedIn* is one of few mergers in which likely effects on privacy competition were found.

To mitigate the privacy-related foreclosure concerns, the Commission required that Microsoft commit to limit the automatic installation of LinkedIn on Window's PCs, both at the manufacturer and end-user level. The Commission required protective measures to prevent

Microsoft from retaliating against manufacturers who choose to install competing social networking applications. It also required Microsoft to provide commitments to ensure continued interoperability between Windows and competing professional social networking services, such as guaranteed competitor access to Microsoft APIs and Microsoft's Graph.

In *Microsoft/LinkedIn*, the Commission also considered, but ultimately dismissed, two other theories of harm that focused on data-combination rather than privacy: i) the potential for horizontal effects in data for online advertising, as both Microsoft and LinkedIn had data sets used for non-search advertising and ii) the potential for vertical input foreclosure effects (in which LinkedIn data was the input) in the market for customer relationship management (CRM) software, if, post-merger, Microsoft denied competitors access to LinkedIn's data for use in customer relationship management software (instead using it exclusively for Microsoft's own CRM products).[277]

The Commission found no likely anticompetitive effects based on either of these data-related theories. First, horizontal effects in online advertising were unlikely, because both of the parties were small competitors in online advertising, there was a large amount of online user data that was not within the merging companies' exclusive control, and neither company supplied advertising data to third parties to any meaningful extent that might be vulnerable to termination post-merger. On the second theory, the Commission found the merged entity would not likely have the ability to foreclose other competitors in CRM software, because LinkedIn lacked a strong market position in that market.[278] The market was highly fragmented such that LinkedIn data was not a competitively important or scarce input for rival CRM suppliers.[279]

In reaching these conclusions, the Commission noted that existing data protection law and the then-impending GDPR would limit Microsoft's ability to access and process the personal data of users after the merger. This assumption that future data processing would need to comply with data privacy law reduced the Commission's concern over the potential for Microsoft to engage in later data-driven foreclosure of competitors.

See:

[277] EC Merger Brief Microsoft/LinkedIn, *supra* note 273 at 1. CRM software is used across various industries to manage customer interactions, organizing data across sources "such as sales, marketing, customer databases, customer service and technical functions." *Id.*

[278] *Id.* at 3.

[279] *Id.*

Eur. Comm'n, *Microsoft/LinkedIn*, Case No. COMP/M.8124, ¶ 180 (Dec. 6, 2016)

Eur. Comm'n Competition Merger Brief M.8124, *Microsoft/LinkedIn*: Big Data and Conglomerate Effects in Tech Markets 5 (May 2017), https://ec.europa.eu/competition/publications/cmb/2017/kdal17001enn.pdf

Though rare now, it is possible that mergers with privacy-based competitive effects will become more common in the future, for several reasons. First, antitrust enforcers are continuing to focus on data-driven competitive effects and on digital markets, in which many business models depend on the processing of personal data. Second, as discussed below, antitrust law reforms in some jurisdictions may make it more likely that mergers require notification to antitrust authorities in advance and may also make it easier for agencies to challenge mergers. Finally, consumer awareness and demand for more privacy protective products and services appears to be growing. Several privacy authorities observe survey evidence that suggests consumers are becoming increasingly privacy-conscious and concerned over the protection of their data. This shift could translate to greater privacy-based competition, and, as a result, more mergers that implicate such competition.

However, the demand-side distortions discussed above will continue to pose a shared challenge across both regulatory realms.[280] Even where consumers declare a growing concern over privacy, those distortions may translate to sub-optimal privacy demand, impacting competition.

As the regulators with the deepest expertise on privacy, privacy agencies can offer valuable insight to antitrust authorities who are seeking to understand and evaluate the effect of mergers on privacy-related competition. Continuing collaboration between antitrust and data privacy agencies will be important both to i) the development of sound overall theories of merger-related privacy effects, and ii) analysis in specific merger reviews. As recent mergers demonstrate, cooperation between antitrust and data privacy agencies can be productive in assessing the likely effects of mergers on privacy-based competition and in the design of merger remedies that are positive for data privacy.[281]

[280] *See* Part I. 4. Shared Policy Interests and Concerns: Trust in Markets, Data Portability and the Impact of Demand-side Distortions in Consumer Choice.

[281] *See* Part II.6. Data Privacy and Antitrust Remedies (discussing the relevance of data privacy to several merger remedies).

a. Jurisdictional Limits and Post-Merger Enforcement Action

As discussed above, the privacy-as-quality theory is viewed by several antitrust agencies as a limitation on their jurisdiction over privacy concerns raised by mergers. This position emerged in response to consumer privacy advocates who regularly pressed antitrust agencies to prevent mergers on the grounds of anticipated harm to the privacy interests of consumers—even where those harms were unrelated to competition.[282] For example, when Facebook acquired WhatsApp, consumer privacy advocates sought antitrust action on the basis that, post-transaction, Facebook would combine and use WhatsApp consumer data in a manner that violated WhatsApp's pre-merger privacy policies.[283] The European Commission considered these arguments, but concluded that "[a]ny privacy-related concerns flowing from the increased concentration of data within the control of Facebook as a result of the transaction do not fall with the scope of EU competition rules but within the scope of EU data protection rules."[284]

The predominant antitrust agency view is that, where privacy is *not* an element of quality-based competition, any privacy effects of a merger are outside of the agency's jurisdiction.[285] "Pure" privacy harms—those unrelated to the likely effects on competition from the merger—are not generally viewed as cognizable in merger review. Where a merger raises privacy and data protection concerns unrelated to competition, such harms are considered the domain of privacy laws and agencies, rather than of antitrust law.[286]

---

[282] Advocates opposed the *Facebook/WhatsApp* merger, *Google/Nest* merger and more recently, Google's acquisition of the fitness data company FitBit. *See* Complaint of Elec. Priv. Info. Cntr. & Cntr. for Digital Democracy, In re: WhatsApp, Inc. (Mar. 6, 2014) (FTC) [*hereinafter* WhatsApp Complaint]; *Google Plans Advertising on Appliances, Including Nest Thermostat*, ELECTRONIC PRIVACY INFORMATION CENTER (May 22, 2014), https://epic.org/2014/05/google-plans-advertising-on-ap.html (urging the FTC to block Google's acquisition of Nest on privacy grounds); Peter Swire, *Protecting Consumers: Privacy Matters in Antitrust Analysis*, CTR. FOR AM. PROGRESS 41 (Oct. 19, 2007), http://www.americanprogress.org/issues/regulation/news/2007/10/19/3564/protecting-consumersprivacy-matters-in-antitrust-analysis/; Jennifer Elias, *Why Google's Fitbit Deal Could Break Its Legacy of Hardware Failures*, CNBC, Nov. 2, 2019 (quoting Congressman David Cicilline as saying "Google's proposed acquisition of Fitbit would also give the company deep insights into Americans' most sensitive information—such as their health and location data—threatening to further entrench its market power online.").

[283] *See, e.g.*, WhatsApp Complaint, *supra* note 282.

[284] Eur. Comm'n, Facebook/WhatsApp, Case No. COMP/M.7217 C(2014) 7239, ¶ 164 (Oct. 3, 2014).

[285] On rare occasions dissenting agency representatives have supported a broader integration of data privacy considerations into antitrust law. *See, e.g.,* Dissenting Statement, Pamela Jones Harbour, Comm'r, Fed. Trade Comm'n, Google/DoubleClick, FTC No. 071-0170, at 10 (2007), https://www.ftc.gov/sites/default/files/documents/public_statements/statement-matter-google/doubleclick/071220harbour_0.pdf (considering "various theories that might make privacy 'cognizable' under the antitrust laws").

[286] Terrell McSweeny, FTC Comm'r, *Big Data: Individual Rights and Smart Enforcement*, Remarks at the European Data Protection Supervisor-BEUC Joint Conference (Sept. 29, 2016).

One of the earliest examples of such reasoning is in the FTC's 2007 review of the *Google/DoubleClick* merger. The FTC observed that this was not the first time the agency had been called upon to block a merger based on non-antitrust concerns, drawing comparisons to demands for antitrust to prevent environmental degradation or protect employees from the effects of mergers.[287] The majority of the FTC Commissioners rejected the idea of using merger review to protect privacy, viewing this as beyond the scope of antitrust law, and thus beyond the agency's jurisdiction (though a dissenting Commissioner would have taken action in response to the alleged data privacy harms).[288] The FTC has continued to take this position since, finding that privacy effects unrelated to competition are beyond the agency's purview.

In its 2006 decision on the *Asnef/Equifax* merger, the European Court of Justice explained similarly that "any possible issues relating to the sensitivity of personal data are not, as such, a matter for competition law, [and] they may be resolved on the basis of the relevant provisions governing data protection."[289] In more recent merger reviews, the European Commission has also taken the view that it is beyond their jurisdiction as an antitrust agency to consider separate data privacy harms that are unrelated to quality-based competition.[290] Other jurisdictions take a similar position on the bounds of antitrust law in their agency guidance.[291]

Merger review and data privacy law may also interact in another way: the European Commission has noted in several mergers that data protection laws are expected to constrain the parties' post-merger access and processing of personal data, and therefore *reduce* the concern over likely post-

[287] FTC Google/Doubleclick, *supra* note 192.

[288] *Id*. at 2 (noting "…the sole purpose of federal antitrust review of mergers and acquisitions is to identify and remedy transactions that harm competition. Not only does the Commission lack legal authority to require conditions to this merger that do not relate to antitrust, regulating the privacy requirements of just one company could itself pose a serious detriment to competition in this vast and rapidly evolving industry.").

[289] Case C-238/05, *Asnef-Equifax,* ECLI: EU: C:2006:734, ¶ 63 (Nov. 23, 2006).

[290] Eur. Comm'n Press Release IP/14/1088, Mergers: Commission Approves Acquisition of WhatsApp by Facebook (Oct. 3, 2014), http://europa.eu/rapid/press-release_IP-14-1088_en.htm ("[a]ny 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 EU competition law."); Eur. Comm'n Press Release IP/20/2484, Mergers: Commission Clears Acquisition of Fitbit by Google, subject to Conditions (Dec. 17, 2020) (investigated potential privacy concerns over ability of users to track how their health data is used, but finding that Google will have to comply with the GDPR and "such concerns are not within the remit of merger control" as "there are regulatory tools better placed to address them").

[291] Singapore, Data: Engine for Growth *supra* note 14, at 13 (resisting calls for competition law to be used to protect privacy as beyond the role and function of the competition authority, but also noting that where data protection is a non-price factor in competition, it may be considered within competition analysis).

merger privacy effects.[292] Where regulatory limits "such as data protection laws" preclude or limit the merging parties' ability to aggregate, access and process user data, those limits can reduce post-merger effects on data-driven competition.[293] Data privacy and protection laws may therefore affect the conclusions drawn in merger analysis regarding the likelihood of anticompetitive effects that involve personal data. However, at least one antitrust agency has also affirmed that the presence of overlapping privacy regulation does not limit its willingness or responsibility to oversee quality-based competition.[294]

This assumption that privacy law will constrain post-merger conduct has proven accurate in at least one merger, where privacy authorities intervened after the data privacy harms predicted during the merger review began to materialize. As mentioned above, in the *Facebook/WhatsApp* merger review, privacy advocates raised concerns over the combination of personal data the merger would enable, but antitrust authorities found that any such harm was beyond their jurisdiction. Two years after Facebook's acquisition of WhatsApp, Facebook updated the applicable terms of service to enable sharing of data with the "Facebook family of companies" for a range of purposes such as marketing and advertising.[295] These purposes were not included when users initially signed-up to the WhatsApp service (in the period before the company was acquired by Facebook). WhatsApp users were provided with 30 days to accept the amended terms or lose access to the WhatsApp online chat service.[296] This planned change triggered attention from the European Article 29 Data Protection Working Party,[297] followed by

[292] *See, e.g.*, Eur. Comm'n, Verizon/Yahoo, Case No. COMP/M.8180, ¶ 90 (Dec. 12, 2016), https://ec.europa.eu/competition/mergers/cases/decisions/m8180_240_3.pdf.; Eur. Comm'n, Microsoft/LinkedIn, Case No. COMP/M.8124, ¶ 179 (Dec. 6, 2016). https://ec.europa.eu/competition/mergers/cases/decisions/m8124_1349_5.pdf.

[293] Eur. Comm'n, Competition Merger Brief M.8124, *Microsoft/LinkedIn: Big Data and Conglomerate Effects in Tech Markets* 5 (May 2017), https://ec.europa.eu/competition/publications/cmb/2017/kdal17001enn.pdf (describing conclusion in Facebook/WhatsApp that privacy was not a major basis for competition).

[294] Competition Bureau Canada Big Data Report *supra* note 68 ("while the Bureau recognizes that other enforcement agencies may have oversight of certain aspects relevant to the quality of goods and services, including privacy, that oversight does not limit the Bureau's responsibility to enforce the Act.").

[295] *See* Info. Comm'r Off., *Blog: Information Commissioner Updates on WhatsApp/Facebook Investigation* (Nov. 7, 2016), https://ico.org.uk/about-the-ico/news-and-events/blog-information-commissioner-updates-on-whatsapp-facebook-investigation/.

[296] *See id.* (noting the 30 day consent window); Letter from Isabelle Falque-Pierrotin, Chairwoman, Article 29 Data Protection Working Party (Oct. 27, 2016), https://www.cnil.fr/sites/default/files/atoms/files/20161027_letter_of_the_chair_of_the_art_29_wp_whatsapp.pdf (noting the amendment was not in the original terms of use for WhatsApp).

[297] Article 29 Data Protection Working Party Letter, *id.* Although antitrust authorities also fined Facebook/WhatsApp after the merger, this was on technical grounds related to the merger filing rather than any substantive privacy concern. Facebook had represented at the time of the merger that it could not establish reliable, automated matching between Facebook user accounts and those of WhatsApp users, when, in fact, the possibility of matching existed and was known at the time of the merger notification. The Commission found, therefore that

enforcement action or investigations in several other jurisdictions, including the U.K., France, Germany, Turkey[298] and Italy.[299]

The U.K. privacy authority, for example, found that WhatsApp had not identified a lawful basis of processing for any such sharing of personal data with Facebook, had failed to provide adequate fair processing information to users.[300] If the data sharing proceeded as planned, it would therefore contravene U.K. data protection law.[301] WhatsApp publicly committed not to share personal data with other Facebook corporate entities until such sharing could be completed in compliance with the GDPR.[302]

One approach to mitigate this type of anticipated privacy harm has been to obtain voluntary commitments from the merging parties to antitrust authorities that specify data will not be combined or used post-merger in the manner that raises privacy concerns.[303] Another approach has been for data privacy authorities to issue warning letters to the merging parties at the time of the transaction, reminding the parties of their obligation to comply with data privacy law post-merger.[304] The FTC's privacy law enforcement division sent this type of letter in the

Facebook had supplied incorrect or misleading information in its merger review filings. Eur. Comm'n, Facebook/WhatsApp, Case No. COMP/M.8228 (May 17, 2017), https://ec.europa.eu/competition/mergers/cases/decisions/m8228_493_3.pdf.

[298] Turkish Competition Authority, *Competition Board Launched an Investigation into Facebook and WhatsApp ex Officio and Stopped the Obligation to Share WhatsApp Data* (Jan. 11, 2021), https://www.rekabet.gov.tr/en/Guncel/competition-board-launched-an-investigat-c9382b8cb15ceb11812900505694b4c6.

[299] The Italian Data Protection Auth. (Garante per la Protezione dei Dati Personali), *Whatspp: New Privacy Policy Unclear, Says the Italian SA* (Jan. 14, 2021), https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9519943.

[300] U.K. Info. Comm'r Off., *Blog: A Win for the Data Protection of UK Consumers* (Mar. 14, 2018), https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2018/03/blog-a-win-for-the-data-protection-of-uk-consumers.

[301] *Id.*

[302] *Id.* In other matters, the U.K. privacy authority has also held acquiring companies accountable for the data breaches or privacy law violations by the acquired company that pre-date the merger. U.K. Info. Comm'r Off., Statement: Intention to Fine Marriott International, Inc More Than £99 Million Under GDPR for Data Breach (July 9, 2019), https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2019/07/statement-intention-to-fine-marriott-international-inc-more-than-99-million-under-gdpr-for-data-breach/ (fining Marriott hotel group for a data breach related to security vulnerabilities that pre-dated its acquisition of Starwood. The ICO's investigation found that Marriott failed to conduct sufficient due diligence when it acquired Starwood and should also have taken further action to secure the acquired systems.).

[303] Eur. Comm'n Press Release IP/20/2484, Mergers: Commission Clears Acquisition of Fitbit by Google, Subject to Conditions (Dec. 17, 2020), https://ec.europa.eu/commission/presscorner/detail/en/ip_20_2484.

[304] Jessica Rich, Dir. Bureau of Consumer Protection, Letter to WhatsApp from the Fed Trade Comm'n, at 2-3, (Apr. 10, 2014).

Facebook/WhatsApp merger. Despite this warning, a subsequent antitrust complaint by state enforcers has alleged that post-merger, the combination of user data across the Facebook and WhatsApp services led to privacy harms (though the specific nature of the harms is not described).[305]

b. Data-Driven Mergers

The value of firms is increasingly driven by their use of data. As a result, mergers with data-driven effects on competition are also increasing. Not all of these data-driven mergers effects will also implicate data privacy—in fact, many will not. However, these general data-related theories are useful to understand, because they have a longer and more familiar history in antitrust analysis than privacy-specific concerns.[306] The more extensive past experience of antitrust authorities with data-driven merger effects may provide a useful starting point in collaborations and discussions with data protection agencies about mergers that impact data privacy.

Antitrust agencies acknowledge that the combination of data as a result of a merger may have pro-competitive effects. Richer sets of post-merger information may enable innovative and improved products or services.[307] There may be data-related efficiencies that arise from the

[305] Complaint, State of New York v. Facebook, Inc., No. 1:20-cv-03589 (D.D.C. Dec. 9, 2020).

[306] *See, e.g.*, Competition Bureau Canada Big Data Report *supra* note 68 (noting "the use of data is hardly new," and refencing analysis of retail, railroad, credit reporting data, airline reservation and financial data); Dir. of Investigation & Rsch v. Air Canada, Reasons for Consent Order (July 7, 1989), http://www.ct-tc.gc.ca/CMFiles/CT -1988-001_0576_45OOJ -4272004 -5490.pdf), http://www.ct-tc.gc.ca/CMFiles/CT -1988-001_0576_45OOJ -4272004 -5490.pdf (requiring merging airlines to make their data available to all computer reservation systems in Canada); Complaint, United States v. Thomson Corp. & Reuters Group PLC ¶ 33-53 (Feb. 19, 2008), https://www.justice.gov/atr/case-document/complaint-222 (alleging merger would harm competition in the supply of financial data); Complaint, FTC v. Dun & Bradstreet, Dkt. No. 9342 (F.T.C., May 7, 2010) (challenge of Dun & Bradstreet acquisition of Quality Education Data included unique data sets on grades K-12 educators); Eur. Comm'n, Google/DoubleClick, Case No. COMP/M.4731, ¶ 90 (Mar. 11, 2008) (considering whether the combination of the firm's data sets would foreclose competition but concluding it would not); Dir. of Investigation and Res. v. D & B Co. of Canada Ltd. (A.C. Nielsen), C.C.T.D. No. 20 (Aug. 30, 1995); Eur. Comm'n Competition Merger Brief M.8124, Microsoft/LinkedIn: Big Data and Conglomerate Effects in Tech Markets, at 5 (May 2017), https://ec.europa.eu/competition/publications/cmb/2017/kdal17001enn.pdf; Comp. Comm'n of Singapore, Notification for Decision: Merger Between the Thomson Corporation and Reuters Group PLC, CCS 400/007/07 (May 23, 2008) (considering the impact of data set concentration on barriers to entry); Eur. Comm'n, TomTom/Tele Atlas, COMP/M.4854 C(2008) 1859, at 41-55 (May 14, 2008) (concluding access to information regarding rivals not likely to create a barrier to competition post-merger); Eur. Comm'n, Thomson Corp./Reuters Grp., COMP/M.4726 C (2008) 654, at 27-28 (Feb. 19, 2008) (finding the proposed merger unlikely to have a significant effect on third-party competitors' access to contribution data contained on the Reuters platform).

[307] Crémer Report, *supra* note 110, at 110-111.

combination of the parties' businesses and data sets.[308]

However, antitrust agencies also acknowledge the potentially negative effects that the combination of data may have on competition. The simplest effects may occur when parties compete using their separate data sets, and that competition is eliminated by the parties' merger. Agencies have also considered a number of more complex data-related merger theories that include:

- Whether the accumulation or combination of data arising from a merger provides a competitive advantage, such as the creation of barriers to entry or expansion of competitors,[309] increased market power,[310] or increased potential for coordinated firm misconduct;[311] and

- Whether data is an input necessary for competition, and, if so, whether the merged parties would have the incentive and ability to limit or foreclose a rivals' access to

[308] Personal Data Protection Comm'n of Singapore & Competition and Consumer Comm'n of Singapore, Discussion Paper on Data Portability ¶ 3.27 (Feb. 25, 2019) (noting potential for data-driven merger efficiencies) [*hereinafter* Singapore Data Portability Discussion Paper].

[309] *See, e.g.*, Competition Comm'n of Singapore, Notification for Decision of the Proposed Acquisition of SEEK Asia Investments Pte. Ltd. of the JobStreet Business in Singapore, CCS 400/004/14 (Nov. 13, 2014) (finding that a merger of employment agency databases concentrated data to create a significant barrier to entry, imposing merger commitments as a condition of approval); Eur. Comm'n, Press Release, *Mergers: Commission Clears Acquisition of Fitbit by Google, Subject to Conditions* (Dec. 2020), https://ec.europa.eu/commission/presscorner/detail/en/ip_20_2484 (finding the combination of Fitbit's health and fitness data with the "already vast amount of data that Google could use for personalisation of ads," raised barriers to advertising rival's entry and expansion in the markets for online search, display advertising and the ad tech ecosystem).

[310] Singapore Data Portability Discussion Paper, *supra* note 308 (the combination of data via a merger may increase the merging parties' market power).

[311] *See, e.g.*, Competition Bureau Canada Big Data Report *supra* note 68, at 21 (discussing the potential for merger effects on competition to be exacerbated where a merger facilitates coordination by making data more readily available or transparent, or removes a competitive constraint on data-driven coordination such as a maverick firm); ACCC Digital Platforms Inquiry Final Report *supra* note 71, at 108 ("For large digital platforms, acquisitions that enhance their already large volume and scope of data may well further entrench their market power and raise barriers to entry and expansion in relevant markets."); Eur. Comm'n, Verizon/Yahoo, Case No. COMP/M.8180, ¶ 81 (Dec. 12, 2016), https://ec.europa.eu/competition/mergers/cases/decisions/m8180_240_3.pdf outlining the main theories for horizonal data combination); Eur. Comm'n, Microsoft/LinkedIn, Case No. COMP/M.8124, ¶ 179 (Dec. 6, 2016), https://ec.europa.eu/competition/mergers/cases/decisions/m8124_1349_5.pdf (outlining the main theories for horizonal data combination).

that data post-merger (vertical foreclosure effects).[312]

In evaluating data-driven effects on competition, an important consideration is often whether the data at stake is unique, and whether the data is within the merging parties' exclusive control.[313] As one FTC enforcer explains:[314]

> The relevant question for antitrust is whether the data of the two firms is a key differentiator and whether other firms that compete with them cannot replace the competition that would be lost from the merger. If that's not the case, then the data itself is not a key driving competitive issue and the fact that the firms have a lot of data is not significant for antitrust analysis.

Several merger decisions have concluded that when the relevant data is replicable from other sources, it is unlikely negative effects on data competition will occur.[315] For example, in the *Microsoft/LinkedIn* transaction, described in **Figure 5. Case Study of the European Commission's Review of the *Microsoft/LinkedIn* Merger** above, the European Commission considered whether the combination of Microsoft and LinkedIn's advertising-related datasets was likely to result in reduced post-merger competition. The agency concluded this was unlikely, since the merging firms were relatively small competitors, and a large amount of online data useful for advertising purposes would remain outside of their control after the transaction.

[312] *See, e.g.*, Competition Bureau Canada Big Data Report 68, at 18 (discussing potential for vertical foreclosure effects where data is an input into the production of goods or services); Eur. Comm'n, Microsoft/LinkedIn, Case No. COMP/M.8124, ¶ 179 (Dec. 6, 2016).

[313] Eur. Comm'n, Microsoft/LinkedIn, Case No. COMP/M.8124, ¶ 180 (Dec. 6, 2016) (finding a large amount of relevant data remained beyond the merging parties control); Eur. Comm'n, Verizon/Yahoo, Case No. COMP/M.8180, ¶¶ 91, 93 (Dec. 12, 2016) (data sets of the merging parties are not unique or exclusively within their control); Crémer Report, *supra* note 110, at 110-111 (noting potential competitive impacts where there is concentration of "control over valuable and non-replicable data resources").

[314] Bruce Hoffman, Acting Dir. Bureau of Competition, FTC, Antitrust in the Financial Sector Remarks at Concurrences 6 (May 2, 2018), https://www.ftc.gov/system/files/documents/public_statements/1408262/hoffman_-_antitrust_in_the_financial_sector_5-2-18.pdf.

[315] *See, e.g.*, *id.* at 2 (discussing merger review of Amazon/Whole Foods, which found the combined data set of the parties was not unique or particularly significant to competition and therefore would not provide a strong competition advantage post-merger); Eur. Comm'n, Microsoft/LinkedIn, Case No. COMP/M.8124, ¶ 180 (Dec. 6, 2016) (large amount of relevant data remains beyond the merging parties control); Eur. Comm'n, Verizon/Yahoo, Case No. COMP/M.8180, ¶ 91, 93 (Dec. 12, 2016) (data sets of the merging parties not unique or exclusively within their control); Facebook/WhatsApp EU (finding that competition for online advertising was unlikely to be impacted by Facebook use of WhatsApp data because the parties were relatively small and a large amount of online advertising data was not within the parties' exclusive control).

Many mergers that involve data-related anticompetitive effects do not raise implications or theories related to privacy. For example, in 2016, the Canadian competition authority considered a merger that enabled the combination of data from a pharmaceutical wholesaler with that of the retail pharmacy chain target.[316] The agency found the merger was likely to substantially lessen or prevent competition, because the merged entity would be able to use the data to better anticipate the behavior of its competitors.[317] However, no theories of privacy harm were considered in the review of this merger. The competitive effects were data-related but not privacy-related.

Even when a merger enables the parties to combine their respective sets of personal data, it is still possible that the transaction will not raise concerns within the remit of competition law. In its review of the recent *Google/Fitbit* merger, the European Commission found that the combination of Google's extensive advertising data with Fitbit's health and fitness data would raise barriers to entry and expansion in various search and advertising markets, likely raising advertising prices and reducing choice for advertisers.[318] In other words, there were data-related effects on competition. However, the Commission considered and dismissed a separate theory that the merger would impact individuals' privacy, by making it more difficult for consumers to track how their health data was being used. The Commission found the privacy concerns "not within the remit of merger control," and noted that Google was obligated to comply with GDPR.[319]

This *Google/Fitbit* merger analysis illustrates an important distinction between data-driven merger effects, which were found (but did not relate to privacy), and theories of standalone privacy harm that are untethered to competition, which the competition authority dismissed as beyond their purview.[320] This is in contrast to *Microsoft/LinkedIn*, where the privacy effects were thought to be *caused by* the likely competitive foreclosure arising from the merger, and therefore considered part of the antitrust harm evaluation. Mergers with data-driven effects are best understood as potentially co-existent, rather than synonymous with, mergers with data privacy

[316] Competition Bureau Canada, Statement Regarding McKesson's Acquisition of Katz Group's Healthcare Business (Dec. 16, 2016), https://www.competitionbureau.gc.ca/eic/site/cb-bc.nsf/eng/04174.html.

[317] *Id.*

[318] Eur. Comm'n Press Release IP/20/2484, Mergers: Commission Clears Acquisition of Fitbit by Google, Subject to Conditions (Dec. 17, 2020), https://ec.europa.eu/commission/presscorner/detail/en/ip_20_2484.

[319] *Id.* (investigated potential privacy concerns over ability of users to track how their health data is used, but finding that Google will have to comply with the GDPR and "such concerns are not within the remit of merger control" as "there are regulatory tools better placed to address them").

[320] *But see* Part II. 6. Data Privacy and Antitrust Remedies (discussing that, despite dismissing data privacy theories of harm related to end users in Google/Fitbit, the European Commission included in the commitments (for approval of the merger) a requirement that Google provide EEA users with "effective choice" to grant or deny the use of their Fitbit health data across other Google services).

effects. Mergers where data drives the effects on competition may not have effects on privacy-based competition, and may not even involve personal data.

c. Reforms of Merger Review Thresholds May Increase the Relevance of Data Privacy

Antitrust agencies in several jurisdictions are focused on the intense, recent merger and acquisition activity by large digital platforms.[321] In particular, there is concern that the acquisitions of nascent rivals may be eliminating important future competitors. This has prompted discussion of whether the competitive effects of such acquisitions may be under-examined, because the transactions fall below the existing size and financial thresholds that trigger pre-merger filing requirements to antitrust authorities.[322] Further, even when such mergers are reviewed, several competition policy reports acknowledge that it may be difficult to assess the effects on competition that will arise from eliminating small but potentially significant future competitors.[323]

In response to these concerns, several jurisdictions are considering proposals for tougher merger enforcement rules.[324] Germany has already amended its competition legislation, changing the thresholds that trigger pre-merger filing and introducing other amendments, all of which are expected to make it easier for German competition authorities to challenge mergers in the digital

[321] Furman Report on Digital Competition, *supra* note 96, at 105 (identifying under-enforcement of merger review in digital markets); Crémer Report, *supra* note 110, at Chapter 6 (examining acquisitions by large digital platforms of start-ups and whether it necessitates changes to EU merger control); ACCC Digital Platforms Inquiry Final Report, *supra* note 71, at 10.

[322] Crémer Report, *supra* note 110, at 111; Furman Report on Digital Competition, *supra* note 96, at 120; ACCC Digital Platforms Inquiry Final Report, *supra* note 71, at 10 (calling for updates to Australia's merger review framework in light of digital concentration enabled through acquisitions).

[323] Crémer Report, *supra* note 110, at 111; Furman Report on Digital Competition, *supra* note 96, at 98 (Mar. 13, 2019) (noting importance and difficultly of assessing potential competition in digital mergers); ACCC Digital Platforms Inquiry Final Report, *supra* note 71, at 10 (recommending that large digital platforms be asked to agree to a merger notification protocol to provide ACCC notice of transactions, which is ordinarily voluntary); Competition Bureau Canada Big Data Report *supra* note 68, (discussing the challenges of evaluating future prevention of competition in data-focused mergers).

[324] ACCC Digital Platforms Inquiry Final Report, *supra* note 71 (proposing changes to notification requirements for large digital platforms under an otherwise voluntary notification system, and to include "potential" competition in assessment and that data may be a competitively important asset); Furman Report on Digital Competition, *supra* note 96, at 95 (proposing merger notification be required for certain digital companies under an otherwise voluntary notification system and changes to substantive merger law to focus more on potential competition); K. Jae-Heun, *KFTC Drafts Policy to Prevent Platform Monopolism*, THE KOREA TIMES (June 29, 2020) (describing proposed Korean legislation that would require merger filings if there is a likely impact on competition from the transaction, regardless of size).

economy.[325] Other jurisdictions are considering potential updates to their antitrust agency guidance to make it more explicit about the analysis of digital mergers and related issues.[326] Still others have concluded that it is too early for legislative changes to pre-merger notification thresholds, but are contemplating whether to revisit the substantive theories of merger harm related to acquisitions of potential future competitors.[327]

Though these developments are not explicitly related to data privacy, their effect may be to impact the likelihood that merger reviews will involve privacy issues. Since personal data plays an important role in many of the digital businesses that provoked these reforms, this newfound scrutiny of their acquisitions may also incidentally increase the number of merger reviews in which privacy-based competition plays a role.

4. Data Privacy Considerations in Abuse of Dominance/Monopolization Analysis

Most jurisdictions around the world prohibit abuse of dominance or "monopolization" in their competition laws.[328] The specifics of those laws and their application vary,[329] but the shared focus is to prevent firms with market power from unilaterally engaging in misconduct that unduly limits competition. Many different practices that harm consumer welfare are recognized as anticompetitive abuses of dominance,[330] but these practices are often grouped into two general categories which are used here: exclusionary conduct and exploitative conduct.

---

[325] *Act Against Restraints of Competition 2013* (Ger.) (as amended in 2017 to include the value of the transaction rather than solely turnover in merger thresholds, and adding new clarifications on platforms and networks). The German competition legislation was further modified in January 2021 to require that transactions involving a small market (referred to as a "de minimus" market) be notified to antitrust authorities and to change the revenue thresholds that trigger merger filing requirements. *Act Against Restraints of Competition 2013 Digitization Act* (Ger.) (2021).

[326] CMA Online Platforms and Digital Advertising Market Study, *supra* note 94, at 95 (proposing review and update of UK merger guidelines); Competition & Consumer Comm'n of Singapore, *Proposed Amendments to the* CCS *Guidelines*, *Consultation Document* (Sep. 10, 2020), https://www.cccs.gov.sg/public-register-and-consultation/public-consultation-items/2020-public-consultation-on-proposed-changes-to-competition-guidelines. (consultation on the addition of privacy and data related amendments to both merger and abuse of dominance guidance).

[327] Crémer Report, *supra* note 110, at 10-11.

[328] Though there are distinctions to be drawn between monopolization and abuse of dominance prohibitions, for simplicity this Report refers to the more common international term of "abuse of dominance" instead of monopolization. This is not intended to exclude concepts of monopolization from the Report discussion.

[329] *See, e.g.*, OECD, Abuse of Dominance in Digital Markets, at 9-12 (2020), http://www.oecd.org/daf/competition/abuse-of-dominance-in-digital-markets-2020.pdf (canvasing differences across jurisdictions in abuse of dominance law).

[330] *See, e.g.*, *id.* at 23 (discussing refusals to deal, predatory pricing, margin squeezing, exclusive dealing, tying, bundling and exploitative abuses as potentially relevant types of abuse of dominance in digital markets, but noting

This section begins by considering the emerging agency views on the relationship between monopoly, competition and privacy at a general level. It then elaborates on theories of abuse of dominance that are the most relevant to data privacy enforcers, in subsections discussing theories of exploitative conduct, and theories of exclusionary conduct. Finally it considers an emerging topic: whether the protection of individuals' data privacy may act as a justification for anticompetitive conduct that would likely otherwise constitute an abuse of dominance.

As this section explains, most abuse of dominance investigations and cases are not expressly focused on data privacy. However, antitrust agencies have paid extensive recent attention to the potential for abuse of dominance in digital markets. A 2020 International Competition Network survey found that 30 of 39 respondent jurisdictions had opened abuse of dominance investigations in digital markets, and at least 17 were taking enforcement action.[331] This digital focus has meant significant recent attention to the role of data in competition and in anticompetitive conduct. This section sets out the few privacy-relevant antitrust theories of abuse, but also discusses these broader data-related theories. The purpose of this broad coverage is to raise cross-doctrinal awareness among privacy authorities, who are often also focused on digital markets and the use of data use.

a. The Relationship Between Monopoly, Competition and Data Privacy

There is not yet a concrete understanding of the relationship, causal or otherwise, between monopoly and data privacy or privacy law. Few abuse of dominance cases have expressly considered privacy. In those that have, privacy is often a minor aspect of the case. The result is that interactions at the juncture between abuse of dominance and data privacy are at a very early stage of development, and largely theoretical or assumed.

When antitrust agencies refer to the connection between monopolization and privacy, it tends to be in portraying market power, or a lack of competition, as a likely cause of low privacy quality or choice for consumers.[332] For example, a recent complaint by U.S. state attorneys general

these categories are not exhaustive in describing forms of anticompetitive conduct and "an openness to considering new types of misconduct may be particularly important in digital markets.").

[331] Int'l Competition Network, Report on the Results of the ICN Survey on Dominance/Substantial Market Power in Digital Markets (July 2020), https://www.internationalcompetitionnetwork.org/wp-content/uploads/2020/07/UCWG-Report-on-dominance-in-digital-markets.pdf.

[332] *See, e.g.*, Furman Report on Digital Competition, *supra* note 96, at 43 ("Although privacy is not directly within the scope of the Panel's review, the misuse of consumer data and harm to privacy is arguably an indicator of low quality caused by lack of competition. It may also be a method for achieving and cementing market power"); U.K. CMA Online Platforms and Digital Advertising Market Study, *supra* note 94, at ¶ 13 (limited choice and

against Facebook, a leading social media company, alleges that once the company achieved monopoly power, it degraded the available privacy protections and options for users.[333] It argues that, due to a lack of meaningful alternatives for personal social networking, users that were dissatisfied with the privacy options had "nowhere else to go."[334] Similarly, the U.S. DOJ is arguing in its monopolization case against Google that, by restricting competition for online search, Google has "reduc[ed] the quality of search . . . on dimensions such as privacy, data protection, and use of consumer data. . . ."[335] The OECD also recognizes the potential for market power to be used by a firm to unilaterally reduce quality "with respect to privacy, data security, advertising content, ease of switching, or any other dimension that determines consumer value."[336] Low privacy quality has been cast by some antitrust authorities as a symptom of abuse of dominance in markets where companies consistently infringe privacy rules without facing competitive constraints in response.[337] Conversely, data privacy agencies have observed that the application of abuse of dominance prohibitions is likely to promote privacy-enhancing services in the relevant market.[338]

---

competition result in individuals being "less able to control how their personal data is used" and "more personal data to platforms than they would like"); OECD, Global Merger Control: OECD Competition Trends, Volume II 2021, at 29, https://www.oecd.org/daf/competition/oecd-competition-trends-2021-vol2.pdf.(noting "a current lack of differentiation among firms in terms of data protection does not necessarily mean that privacy is not a valued dimension of quality for consumers; indeed, it may instead suggest a lack of competition in the market.").

[333] Complaint, State of New York v. Facebook, Inc., No. 1:20-cv-03589 (D.D.C. Dec. 9, 2020) at ¶¶ 235-244 (describing the alleged erosion of user privacy protection after achieving monopoly power, including through the collection of data about users both on and off of the Facebook social media platform and "pushing users to make more information public").

[334] *Id.* at ¶ 242.

[335] Press Release, U.S. Dep't of Justice, *Justice Department Sues Monopolist Google for Violating Antitrust Laws* (Oct. 20, 2020); *see also* Complaint, State of New York v. Facebook, Inc., No. 1:20-cv-03589 (D.D.C. Dec. 9, 2020) (alleging that, once Facebook obtained monopoly power the company "degraded the privacy protections and privacy options" that had led to its initial popularity over social networking rivals).

[336] OECD, Zero-Price Markets – Background Note, *supra* note 9, at 14.

[337] Peter Hustinx, EDPS, Data Protection and Competition: Interfaces and Interaction at the Data Protection Law in the Context of Competition Law Investigations (June 13, 2013) ("One could also consider that the behaviour of a company which can afford to constantly infringe privacy rules to the detriment of data subjects, without suffering competitive constraints from other competitors, could be considered as an element in the evaluation of dominance. In other words, disrespect for data protection rules could be conceived as a 'symptom' of dominance."); Furman Report on Digital Competition, *supra* note 96, at 43 (noting but not necessarily adopting the view that "it has been argued that these new, firmer boundaries [of GDPR] could support the position of the incumbents, as potential rivals will (rightly) face more restrictions than the incumbents themselves faced in their infancy.").

[338] *See, e.g.*, EDPS, Privacy and Competitiveness in the Age of Big Data: The Interplay Between Data Protection, Competition Law and Consumer Protection in the Digital Economy (March 2014), French Autorité de la Concurrence & Bundeskartellamt, Competition Law and Data Report, at 26 (May 10, 2016) (noting the application of competition rules to digital markets has the "potential to promote privacy-enhancing services").

Such views seem consistent with the "privacy-as-quality" theory described above.[339] Though monopoly power generally confers the ability to profitably raise prices independent of market forces, in theory it could also provide the power to cause a decline in quality—including privacy quality. By this logic, improved competition would be expected to raise the quality of privacy protection in markets where privacy features or products are the basis for competition. The reality may be more complex, given the recognized challenges consumers face in making privacy choices and their potential effects on privacy-related competition.[340]

A privacy-as-quality abuse theory has not been applied in any adjudicated agency cases that were part of the research for this Report, though some cases are beginning to allege similar arguments, as in the Facebook and Google complaints discussed above. The research for this Report found no agency references to empirical evidence that would substantiate such a view, or any potential alternative theories, about the relationship between monopolization and privacy. Whether and when competition or monopoly is likely to lead to greater privacy benefits for consumers is an important question worthy of consideration by both privacy and antitrust authorities. The answers are likely to be affected by issues discussed in other sections of this report, such as demand-side distortions, which may lead to sub-optimal privacy competition.[341]

Several antitrust agencies acknowledge another possible relationship between privacy and monopoly: privacy laws that are difficult to comply with may contribute to the entrenchment of existing monopolists. A prior U.S. Attorney General explains this perspective, indicating that "[o]verbroad and overly burdensome privacy legislation could inhibit competition by entrenching monopolists with the resources to comply, while thwarting newer entrants who do not have those resources."[342] There is some concern that larger firms may be advantaged in privacy compliance relative to smaller competitors who often have fewer compliance resources. In its two-year retrospective of the GDPR issued in 2020, the European Commission notes that "[s]ome stakeholders report that the application of the GDPR is challenging especially for small and medium sized enterprises (SMEs)," though the specific challenges are not described.[343]

---

[339] *See* Part II. 1. Integrating Data Privacy into Antitrust Analysis: The "Privacy-as-Quality" Theory.

[340] *See* Part I.4.c. Consumer Choice and the Challenge of Demand-Side Distortions.

[341] *See id.*

[342] William P. Barr, U.S. Att'y Gen., Remarks at the National Association of Attorneys General 2019 Capital Forum, Washington, D.C. (Dec. 10, 2019); *see similarly* FTC, *Hearings on Competition and Consumer Protection in the 21st Century, Hearing No. 12: The FTC's Approach To Consumer Privacy* 132 (Apr. 10, 2019) (remarks by FTC Commissioner Rebecca Kelly Slaughter) ("We must take care that in attempting to secure increased protection for consumer data privacy, we don't inadvertently further entrench incumbents or otherwise hinder competition and choice," but noting that this concern is commonly expressed by those who oppose new privacy laws).

[343] Eur. Comm'n, Communication from the Commission: Data Protection as a Pillar of Citizens' Empowerment and the EU's Approach to the Digital Transition - Two Years of Application of the General Data Protection Regulation,

Research for this Report did not find agency reference to evidence that supports the view that onerous privacy law entrenches incumbent firms.

The European Commission goes on to explain that, despite the potential challenges of privacy compliance for SMEs, it would be inappropriate to provide exceptions to privacy obligations based on the size of a business, because the risk of privacy harm to consumers does not necessarily correlate with firm size.[344] Instead, the Commission notes that efforts are underway to provide practical GDPR compliance resources and assistance to small and medium enterprises, and calls for more of the same.[345]

The Commission's comments reflect a significant theoretical difference between privacy law and the law of abuse of dominance. While abuse of dominance is premised on market power (the ability to raise prices or profitably lower quality from the level that would occur in a competitive market), the application of data privacy law is not expressly dependent on the position of the enterprise in the market; privacy obligations apply to all entities, regardless of their size or power.

In practice, this difference between the two areas of law may be less significant. Data privacy law does not explicitly depend on market power, but the EDPS has described it as "scalable in proportion to the volume, complexity and intrusiveness of a company's personal data processing activities, and . . . therefore of particular relevance to powerful, big data-managing companies."[346] In other words, large, data-driven companies are more likely to have high volume, complex and possibly more intrusive data processing that renders data privacy law of particular relevance. In fact, the EDPS expressly analogizes the heightened relevance of data privacy enforcement to large entities to the special responsibility to avoid the distortion of competition that is imposed on dominant companies in European law.[347] At a practical level, large, data-driven digital companies are likely to be common enforcement priority as privacy agencies seek to allocate their resources to greatest effect. This explains at least in part why data

COM/2020/264, at 9 (June 24, 2020), https://eur-lex.europa.eu/legal-zcontent/EN/TXT/PDF/?uri=CELEX:52020DC0264&from=EN.

[344] *Id.*

[345] *Id.*

[346] European Data Protection Supervisor, Preliminary Op. of the Eur. Data Protection Supervisor, Privacy and Competitiveness in the Age of Big Data 14 (March 2014), https://edps.europa.eu/sites/edp/files/publication/14-03-26_competitition_law_big_data_en.pdf; French Autorité de la Concurrence & German Bundeskartellamt, Competition Law and Data Report, at 14 (May 10, 2016); M.M. v United Kingdom, 24029/07 Eur. Ct. H.R 200 (2012) (commenting in regard to criminal record data that " . . . the greater the scope of the recording system, and thus the greater the amount and sensitivity of data held and available for disclosure, the more important the content of the safeguards to be applied at the various crucial stages in the subsequent processing of the data.").

[347] *Id.*

privacy and antitrust enforcement are increasingly intersecting—both focus on large, powerful, data-driven companies in the marketplace.

Finally, another facet of this monopoly/privacy relationship is the power and control that large digital companies exert over online environments, which has become a subject of concern for both privacy and competition authorities. By virtue of their central position in the digital ecosystem, many dominant firms develop the rules and act as the referees for permitted and prohibited conduct on, and access to, popular websites and other platforms. For example, Amazon controls its popular online marketplace where third-party merchants sell their goods, Google controls what appears in online search and search advertising on its widely-used search engine, and Apple controls access to its app store where both Apple and third parties offer applications for their mobile devices. Facebook, Twitter and other social media platforms act as moderators to determine the content permitted on their services. Each company creates and enforces the terms and conditions of access to their sites of digital commerce, dictating who and what is permitted on these major platforms. Several antitrust agencies refer to this as the online "gatekeeper" function of digital platforms.[348] Though the term "gatekeeper" has no settled or legal meaning, it has become commonly used to refer to this quasi-regulatory role digital platforms often play in controlling access to popular sites of online competition.

This control enables the companies to police misconduct in a manner that can protect users and other participants, by limiting access or barring those who fail to comply with the platform's rules. One enforcer describes the negative flipside of this, casting digital platforms as "so dominant that they're effectively private regulators, with the power to set the rules for markets that depend on those platforms."[349] It is certainly true that these rules, and how they are enforced, may impact both data privacy and competition in the online environment. See, for example, the discussion below of "self-preferencing," which suggests that large digital companies may give preferential treatment to their own vertically-integrated products or services with respect to both privacy obligations and competition.

[348] ACCC Digital Platforms Inquiry Final Report, *supra* note 71 (noting several jurisdictions express concern over gatekeeping function of large platforms in the digital economy); Furman Report on Digital Competition, *supra* note 96, at 41, 47-48; Margrethe Vestager, Comm'r of Competition, Eur. Comm'n, Keeping the EU Competitive in a Green and Digital World, Remarks at the College of Europe, Bruges, (Mar. 2, 2020), https://ec.europa.eu/commission/commissioners/2019-2024/vestager/announcements/keeping-eu-competitive-green-and-digital-world_en.

[349] Vestager, *id.* ("We may still find ourselves dealing with digital platforms that have become so dominant that they're effectively private regulators, with the power to set the rules for markets that depend on those platforms."),; *see also* Crémer Report, *supra* note 110, at 71 (observing "platforms act as regulators of the interactions they host").

For both antitrust and data privacy, the power that platforms exert over digital ecosystems often amounts to a generalized policy consideration or starting point for analysis rather than a violation of either area of law in itself. In most jurisdictions, acting as a gatekeeper is not a violation of antitrust law, thought the term brings with it a connotation of dominance, and the power to exclude rivals from important loci of online competition. An exception to this is German competition legislation, which was amended to create a new antitrust violations that applies only to companies with the status of "paramount significance for competition," akin to that of a gatekeeper.[350] At the EU level, there is also new legislation specific to digital markets that will create regulatory obligations (beyond that of antitrust or privacy law) that are imposed on large digital platforms.[351]

This policy concern over digital platform power also raises questions about the balance between competition and data privacy in digital environments. Pressed by growing privacy compliance obligations, multiple large platforms have made high-profile moves toward "walled garden" business models that increase their control over consumer data, and sequester that data within their technological ecosystems.[352] For example, in January 2020 Google announced plans to phase out third-parties cookies access on is Chrome web browser within two years. Advertisers and publishers currently have access to such cookies, and rely on them to deliver online advertising.

Both privacy and competition agencies are watching closely as Google makes this change.[353] On the privacy side, there is some cautious optimism that the blocking of cookies may signal broader

[350] Fed. Cartel Off. (Bundeskartellamt) (Ger.), Amendment of the German Act Against Restraints of Competition (Jan. 19, 2021), https://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2021/19_01_2021_GWB%20Novelle.html (discussing the new section 19(a) in German competition legislation).

[351] EDPS, Opinion 2/2021, Digital Markets Act (Feb. 10, 2021); EDPS, Opinion 1/2021, Digital Services Act (Feb. 10, 2021).

[352] See discussion in-text of Google third-party cookies termination; John Thornhill, *Apple's Move To Increase Privacy Strengthens Its Walled Garden,* FINANCIAL TIMES (March 18, 2021), https://www.ft.com/content/e4b2ff3b-1fb9-4f6b-837a-ab0368fb7125 (discussing Apple's new operating system which will present users with more options to control in-app tracking).

[353] CMA Online Platforms and Digital Advertising Market Study, *supra* note 94, at ¶ 5.328; ACCC Digital Platforms Inquiry Final Report *supra* note 71, at 135-36 (discussing Google third-party cookies change and noting it "may have positive privacy effects for consumers" but reserving judgment on whether the change is likely to have a material impact on competition, since it has not yet occurred); U.K. Info. Comm'r Off., *Blog: Adtech - The Reform of Real Time Bidding Has Started and Will Continue* (Jan. 17, 2020), https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2020/01/blog-adtech-the-reform-of-real-time-bidding-has-started/; *see also* Transcript, H. Subcomm. on Antitrust, Commercial, and Administrative Law, *Hearing on Online Platforms and Market Power, Part 6: Examining the Dominance of Amazon, Apple, Facebook, and Google*, 116th Cong., at 124 (July 29, 2020) (Rep. Armstrong questioning of Alphabet, Inc. CEO Sundar Pichai regarding the competition impacts of the cookies termination announcement, but acknowledging the potentially countervailing privacy benefits).

change toward more privacy-protective models within the online advertising ecosystem.[354] The likely privacy effects, whether positive or otherwise, will ultimately depend on the alternative technology that Google introduces to replace third-party cookies. Privacy agencies are carefully assessing Google's proposed alternatives.[355]

Antitrust authorities view Google's changes as more uniformly negative for competition. Several states have brought a joint antitrust complaint alleging that, among other claims, Google's third-party cookie changes will contribute to the company's unlawful monopolization of ad buying and exchange markets.[356] This early-stage case is discussed in more detail below.[357] In short, the change eliminates direct access to competitively-important cookie data, which advertisers and publishers currently use to compete with Google in ad delivery and ad tracking.[358] The concern is that this shift will tighten Google's control over ad data, insert Google into the ad supply chain as a new and necessary intermediary for its competitors, and ultimately raise barriers to competition.[359] The U.K. competition authority has expressed similar concerns, and has opened an investigation into Google's plans to terminate third-party cookies on Chrome that involves discussion with the U.K. privacy authority.[360]

Google's cookie change highlights the different policy perspectives of antitrust and data privacy, and the potential for tension between them in the digital economy. Though somewhat simplified, the agency responses to Google so far illustrate that competition policy tends to encourage the flow of data in digital environments, as a means to promote data-driven competition, while data privacy policy often leans toward added controls or limits on such data flow.

[354] Info. Comm'r Off., *id.* The U.K. Information Commissioners Office is also conducting a broader investigation into the adtech industry, *see* Press Release, Info. Comm'r Off.,Adtech Investigation Resumes (Jan. 22, 2021).

[355] *Id*.; U.K. Info. Comm'r Off. & CMA, Competition and Data Protection in Digital Markets: A Joint Statement Between the CMA and the ICO (May 19, 2021) at 29 (noting the U.K. privacy authority is assessing Google's proposed alternative, termed "Privacy Sandbox").

[356] Amended Complaint, Texas v. Google LLC, No. 4:20-cv-957-SDJ (E.D. Tex. March 15, 2021) at 96-99.

[357] *See* Part II.4.b.ii. Theories of Competitive Foreclosure and "Self-Preferencing

[358] *Texas Google Complaint*, *supra* note 356; *See similarly* CMA Online Platforms and Digital Advertising Market Study, *supra* note 94, at ¶ 5.328; ACCC DPA 2019, *supra* note 71 at 135-36.

[359] *Google State Complaint*, *supra* note 356.

[360] Press Release, CMA, CMA to investigate Google's 'Privacy Sandbox' Browser Changes (Jan. 8, 2021) (investigating Google's proposals to remove third-party cookies and other functionalities from its Chrome browser, including whether the proposed changes could cause advertising spend to become more concentrated on Google's ecosystem, reducing competition).

This policy tension presents an opportunity for productive discussion and collaboration between antitrust and data privacy authorities.[361] First, it may be helpful to identify and understand whether (and when) there are truly policy choices or tradeoffs between the promotion of competition and the protection of data privacy. It may be that on closer examination, the interests are not in opposition, and both can be pursued. One antitrust agency speculates that, in some instances privacy and competition interests may coincide over the long term, if the concentration of personal data among few providers eventually *reduces* consumer choice and control over privacy.[362]

Second, to the extent tradeoffs are thought to exist between the two interests, it would be helpful for antitrust and data privacy authorities to jointly discuss how each realm views the appropriate and productive balance between the promotion of privacy and competition. The U.K.'s cross-agency consideration of the Google cookies change is an example of this type of collaboration. Though there are likely to be justified and logical differences in the views of each agency, the discussion remains useful to promote deliberate and careful cross-doctrinal understanding—without this collaboration, there may be unwitting or unintentional tradeoffs, where one realm pursues its interests at the cost of the other. In the absence of shared agency thinking on this subject, digital platforms will be left with the power and ability to decide the balance between data access that promotes competition, and data control that protects privacy.

b. Exclusionary Abuse of Dominance Theories

Most abuse of dominance cases involve exclusionary conduct. The prohibited types of conduct vary, but each involves a dominant company that unilaterally forecloses actual or potential competitors by means other than competition on the merits. As with all abuses of dominance, the misconduct must have an effect on overall competition in a relevant market sufficient or substantial enough to meet the required threshold in law. Exclusionary conduct that reduces competition is thought to harm consumers, by enabling the monopolist to charge higher prices, reduce output or reduce quality. This section considers several data-related theories of abuse of dominance being examined by antitrust authorities, and their potential relevance to data privacy.

i. Data-Focused Theories of Abuse of Dominance

[361] CMA Online Platforms and Digital Advertising Market Study, *supra* note 94, at ¶ 5.330 (noting the same).

[362] *Id.* at ¶ 5.328.

Data-related theories of abuse of dominance are not new,[363] but such theories have seen renewed antitrust attention with the rise of the digital economy and its many data-driven business models. Though some of these cases implicate privacy, many do not.[364] Antitrust authorities are focused on the competitive effects of the conduct, regardless of whether the data is personal.

As a preliminary matter, antitrust authorities have considered whether the scale and scope of data accumulation may act as a barrier to entry and limit competition.[365] Data accumulation is not itself an abuse, and, in fact, may contribute to the very product and service improvements and competition that antitrust seeks to promote.

Instead, the essential element that creates an antitrust law violation is some form of misconduct that constitutes the abuse of dominance. This includes the many types of recognized misconduct described below. In other words, it is the conduct, not the mere involvement of data in that conduct, that raises the antitrust concern. In addition, to violate antitrust law the conduct must have a sufficiently negative effect on competition. If a monopolist excludes certain rivals by engaging in the conduct like that described below, but those actions have minimal or no impact on overall competition, there is no violation of antitrust law. With those caveats, the following are different data-related theories of exclusionary conduct that have been considered in multiple jurisdictions:

- **Exclusion of rivals from important sources of data collection, through the use of exclusivity agreements with buyers or suppliers.**[366] For example, a U.S. DOJ Antitrust Division complaint against Google alleges that the company excluded

[363] *See, e.g.*, Director of Investigation and Research v. D&B Companies of Canada Ltd. (A.C. Nielsen) (1994) (abuse of dominance claiming defendant denied rivals access to retail scanner data through exclusivity agreements); Joined Cases C-241/91 P and C-242/91, RTE and ITP v Comm'n. (Magill), 1995 ECR I-743 (refusal to supply weekly schedule information for television channels); Case C-418/01, IMS Health GmbH & Co. OHG v. NDC Health GmbH & Co. KG, 2004 E.C.R. I-5039 (abuse of dominance involving refusal to license the structure of sales data for pharmaceutical products), https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:62001CJ0418&from=EN.

[364] *See, e.g.*, Competition Bureau, Statement Regarding Its Investigation into Alleged Anti-Competitive Conduct by TMX Group Limited (Nov. 21, 2016), https://www.competitionbureau.gc.ca/eic/site/cb-bc.nsf/eng/04157.html (abuse of dominance investigation into whether TMX's contractual clauses with investment dealers precluded new entrants from obtaining the required volume of securities market data, reducing competition); Case T-201/04, Microsoft Corp. v. Comm'n, 2007 E.C.R. II-3601 (Microsoft abused its dominance through a refusal to supply interoperability information and technical tying of products).

[365] *See* Part II.2.b. Market Power: The Role of Data and Network Effects.

[366] *See, e.g.*, French Autorité de la Concurrence & German Bundeskartellamt, Competition Law and Data Report, at 19 (May 10, 2016) (describing a data-driven exclusive contracts strategy), https://www.bundeskartellamt.de/SharedDocs/Publikation/DE/Berichte/Big%20Data%20Papier.pdf;jsessionid=E302798FED37AC362CE2A36312543392.2_cid390?__blob=publicationFile&v=2.

competitors from obtaining the scale of search data necessary to compete, by entering into distribution agreements that ensured pre-installation of a bundle of Google apps, and the pre-setting of Google search as the default search access point on an array of computer and mobile devices.[367]

Another example arose in an earlier investigation into Google's search practices, in which the Competition Bureau Canada and other global antitrust authorities considered whether Google's exclusive agreements with websites and smartphone manufacturers foreclosed search rivals by denying them access to an adequate volume search query data to compete effectively.[368] The Bureau concluded that Google's agreements lacked the requisite effects on competition for a violation of antitrust law.[369]

- **Bundling or tying of products or services that buyers would not otherwise purchase together, in a manner that reduces competition**.[370] For example, the U.K. CMA describes the potential for a company holding a valuable data set to tie access to that data to the purchase of the company's data analytics services, making it difficult for rivals to compete to provide their own data services.[371] The European Commission has issued a preliminary opinion that Apple violated abuse of dominance prohibitions with its app store rules, which make the use of Apple's in-app purchasing software mandatory for many apps.[372] App developers are charged a significant fee for purchases made using this software, benefitting Apple. The rules also restrict app developers from steering consumers toward alternative purchasing options. Apple's competitors for music streaming have also complained that this tying of Apple's in-app purchasing software disintermediates them from "important consumer data" that

[367] Complaint at ¶¶ 52-57, U.S. Dept. of Justice v. Google, No. 1:20-cv-03010 (D.D.C. Oct. 20, 2020) (summarizing allegations of Google's exclusionary agreements).

[368] Competition Bureau Canada, Competition Bureau Statement Regarding Its Investigation into Alleged Anti-Competitive Conduct by Google (Apr. 19, 2016), https://www.competitionbureau.gc.ca/eic/site/cb-bc.nsf/eng/04066.html (analyzing Google's search syndication and distribution agreements).

[369] *Id.*

[370] *See, e.g.*, *id.* (considering whether Google's bundling of incentives to advertisers to use Google ad exchange and other ad services exclude competition, but finding no anticompetitive effects).

[371] CMA, The Commercial Use of Consumer Data: Report on the CMA's Call for Information (June 2015) at 90, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/435817/The_commercial_use_of_consumer_data.pdf.

[372] Eur. Comm'n Press Release IP/21/2061, Antitrust: Commission sends Statement of Objections to Apple on App Store Rules for Music Streaming Providers (Apr. 30, 2021), https://ec.europa.eu/commission/presscorner/detail/en/ip_21_2061

only Apple obtains regarding the in-app purchases.[373] The Commission's investigation is ongoing as of writing. The U.K. competition authorities are conducting a similar investigation into Apple's app store practices.[374]

- **Leveraging of a monopoly from one market where the dominant firm has market power into an adjacent market.** For example, in 2020, the European Commission reached a preliminary conclusion that Amazon had extended its dominance in certain European national markets by using the company's preferential access to third-party retailer data from Amazon Marketplace.[375] Amazon competes with the third-party sellers on its online Marketplace to sell its own, Amazon-branded retail goods. Amazon allegedly used its privileged position as the operator of this leading online marketplace to access non-public, third-party seller data, which it then used strategically to develop and select new Amazon retail products for sale. The Commission found that this practice enabled Amazon to "avoid the normal risks of retail competition," leveraging its dominant Marketplace to "marginalise" third-party sellers.[376]

Finally, some jurisdictions have raised the possibility that certain data could constitute an "essential facility" to which rivals require access to compete.[377] It is important to note that competition law does not generally impose a general duty to deal with rivals.[378] Even monopolists are free to choose their trading partners. However in certain narrow circumstances, a

[373] Eur. Comm'n Press Release IP/20/1073, Antitrust: Commission Opens Investigations into Apple's App Store Rules (June 16 2020), https://ec.europa.eu/commission/presscorner/detail/en/ip_20_1073.

[374] Press Release, CMA, CMA Investigates Apple Over Suspected Anti-Competitive Behaviour (Mar. 4, 2021) (investigating whether Apple used its dominance to impose unfair or anti-competitive terms on developers who use the company's App Store, resulting in less choice or higher prices for apps).

[375] Eur. Comm'n Press Release IP/20/2077, Antitrust: Commission Sends Statement of Objections to Amazon for the Use of Non-public Independent Seller Data and Opens Second Investigation into Its E-commerce Business Practices (Nov. 10, 2020), https://ec.europa.eu/commission/presscorner/detail/en/ip_20_2077.

[376] *Id.*

[377] *See, e.g.,* EDPS, Privacy and Competitiveness in the Age of Big Data: The Interplay Between Data Protection, Competition Law and Consumer Protection in the Digital Economy (March 2014); French Autorité de la Concurrence and German Bundeskartellamt, Competition Law and Data Report, at 26 (May 10, 2016) (noting "[t]he information [held by digital platforms] could in theory be considered an essential facility in a particular digital market"); *See also* Jason Furman *et al.*, Report of the Digital Competition Expert Panel: Unlocking Digital Competition, at 9 (Mar. 13, 2019) (not referencing the essential facilities theory, but noting that [t]here may be situations where opening up some of the data held by digital businesses and providing access on reasonable terms is the essential and justified step needed to unlock competition").

[378] *See, e.g.,* Verizon Commc'ns Inc. v. Law Offices of Curtis V. Trinko, LLP, 540 U.S. 398, 408 (2004) (quoting United States v. Colgate & Co., 250 U.S. 300, 307 (1919) (parties may freely to exercise their own independent discretion as to whom they will deal).

dominant firm's refusal to deal with rivals in a manner that significantly impacts competition may constitute a violation of antitrust law.[379]

The "essential facilities doctrine" is the most commonly raised of these narrow circumstance when a dominant firm may be obligated to deal with rivals. An essential facility has been described in European law as a product or service that is i) objectively necessary to be able to compete effectively, ii) for which there is no alternative product or service, and iii) where technical, legal or economic obstacles make it impossible or unreasonably difficult to develop an alternative.[380] As this description suggests, the essential facilities theory or doctrine in law applies in the specific situation where access to such facility is required to compete, the facility is extremely difficult for rivals to replicate, and the refusal of access is not otherwise justified.[381]

Essential facilities cases have historically involved physical infrastructure, but now some jurisdictions are applying the doctrine to data,[382] or recognizing the potential do so in policy discussions.[383] Since data, by its nature, is generally a non-rivalrous resource (meaning the same data can be used by multiple firms), an important question in such cases is whether the rival could replicate the data itself in order to compete, rather than relying on access to the dominant firm's data set. The role of data in a particular market would need to be examined on a case-by-case basis.

Competition guidance and law in select jurisdictions have recognized the potential for data to be the subject of an essential facilities claim. Singapore's competition authority recently engaged in a consultation process on proposed amendments to its abuse of dominance guidance.[384] The contemplated changes include clarification that a dominant company's refusal to provide "key inputs," including "data," could violate Singapore's abuse of dominance prohibitions.[385] The

[379] *See, e.g.,* French & German Competition Law and Data Report, *supra* note 377 at 17-18 (discussing a refusal of access to data as anticompetitive where the data constitutes an "essential facility").

[380] *See*, *e.g.*, Case C-418/01, IMS Health GmbH & Co. OHG v. NDC Health GmbH & Co. KG, 2004 E.C.R. (describing the requirements for an essential facilities claim); Case C -7/97, Bronner v. Mediaprint Zeitungs 1998 E.C.R.

[381] *See* discussion in cases cited at *id.*

[382] *See, e.g.*, Case C-418/01, IMS Health GmbH & Co. OHG v. NDC Health GmbH & Co. KG, 2004 E.C.R. (applying essential facilities theory to a refusal to license the structure of sales data for pharmaceutical products).

[383] French & German Competition Law and Data Report, *supra* note 377 at 17 (describing a refusal of data access as anticompetitive where that data is an essential facility).

[384] Competition & Consumer Comm'n of Singapore, *Proposed Amendments To The* CCS *Guidelines*, *Consultation Document* (Sep. 10, 2020), https://www.cccs.gov.sg/public-register-and-consultation/public-consultation-items/2020-public-consultation-on-proposed-changes-to-competition-guidelines.

[385] *Id*. at Annex C, 38-39 (proposed amendments to guidelines on section 47 Abuse of Dominance prohibitions).

guidance would retain the requirements of substantial harm to competition from the refusal, and that duplication of the facility be "impossible or extremely difficult" in order to qualify as "essential."[386] For many types of digital data and data sets, the latter requirement may be particularly difficult to meet. Recent amendments to Germany's competition legislation also revive the essential facilities doctrine specifically for data, stipulating that an abuse of dominance may occur when certain dominant firms refuse to grant access to data that is required to compete.[387] This and other amendments to German competition legislation are unique in their specificity to data and digital markets.

In other jurisdictions, such as the U.S., antitrust agencies are more skeptical of data-driven abuse of dominance, and essential facilities theories in particular.[388] Instead, their emphasis has tended to be on the widely available and inexpensive nature of data online for those who wish to compete, data's non-rivalrous nature (meaning the same data can be used and shared with multiple firms), and the role of other inputs like labor, expertise and capital—not data alone—in creating competitive value.[389]

The greater willingness of European and other jurisdictions to consider essential facilities theories reflects fundamental differences not only in their view of the role of data, but also the applicable antitrust law. Although U.S. agency officials have acknowledged the theoretical possibility that data could constitute an essential facility,[390] their view is that "[i]t is unlikely that this set of facts would violate U.S. law," as U.S. law imposes no duty on monopolists to deal with or assist rivals.[391] U.S. decisions have cast significant doubt on the viability of the essential

[386] *Id.* at 39.

[387] Fed. Cartel Off. (Bundeskartellamt), Amendment of the German Act Against Restraints of Competition, at § 19 (Jan. 19, 2021), https://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2021/19_01_2021_GWB%20Novelle.html (describing amendments to German competition law); Amendments to the Competition Act (GWB) by Article 10 of the Act of 12 July 2018, Federal Law Gazette I (English translation by the Language Service of the Bundeskartellamt) at 1151, ¶20, http://www.gesetze-im-internet.de/gwb/index.html (refusal to grant access to data for a reasonable fee may constitute an abuse of dominance).

[388] Makan Delrahim, Asst. Att'y Gen., U.S. Dept. of Justice, "Start Me Up": Start-Up Nations, Innovation, and Antitrust Policy, Remarks at the University of Haifa in Israel (Oct. 17, 2018), https://www.justice.gov/opa/speech/assistant-attorney-general-makan-delrahim-delivers-remarks-university-haifa-israel; Bruce Hoffman, Acting Dir. Bureau of Competition, U.S. Fed. Trade Comm'n, Antitrust in the Financial Sector Remarks at Concurrences 7 (May 2, 2018) (expressing skepticism of the viability of essential facilities claims regarding data).

[389] Delrahim, *id.*

[390] Hoffman, *supra* note 388 at 7 (". . . there could be a very narrow set of circumstances that could support a potential claim. For example, rivals could assert that the firm's data amounted to an 'essential facility.'").

[391] *Id.*; *See similarly* Delrahim, *supra* note 388 ("In the United States, however, we do not generally require firms, even dominant ones, to deal with competitors. I am not yet convinced that we should have different rules for data.").

facilities doctrine, although none have expressly eliminated it.[392] This jurisprudence makes it unlikely that U.S. federal antitrust agencies would bring a case featuring arguments that data is an essential facility.

In addition to these legal differences, the specific facts of each case will play an important role in theories of data-driven misconduct. This includes considerations such as: the specific nature of the data at stake, its role in competition and whether the data at issue could be effectively replicated by competitors. A fundamental, and often difficult, question will be whether the data-related effects are the result of product improvement on the merits—which antitrust law encourages—or instead constitute an abuse of market power, which antitrust law prohibits.

ii. Theories of Competitive Foreclosure and "Self-Preferencing"

In a new variation on traditional antitrust theories, several agencies have expressed concern that competition will suffer where large digital platforms use their "gatekeeper" status to self-preference—to advantage their own vertically integrated products and services over those of rivals.[393] "Self-preferencing" is a term of art used in digital policy discussions, particularly in European jurisdictions, to refer to a certain type of exclusionary conduct premised on the dual role of many digital giants, who act as both i) the "gatekeepers" or operators of the sites where online competition occurs, and ii) as competitors to third-parties who rely on access to the gatekeeper-controlled sites to sell their own products or services. The allegation is that this dual role is being used to engage in anticompetitive conduct.

[392] Hoffman, *supra* note 390; Verizon Commc'ns Inc. v. Law Offices of Curtis V. Trinko, LLP, 540 U.S. 398, 411 (2004) (noting the U.S. Supreme court has never recognized the essential facilities doctrine and finding it inapplicable where state or federal regulation could compel facilities sharing, but declining to repudiate the doctrine entirely).

[393] *See, e.g.,* European Comm'n, Commission Opens Investigation Into Possible Anti-Competitive Conduct Of Amazon (July 17, 2019), https://ec.europa.eu/commission/presscorner/detail/en/IP_19_4291 (investigating Amazon's business practices in its "dual role as marketplace and retailer"); ACCC Digital Platforms Inquiry Final Report, *supra* note 71, at 12 ("Google and Facebook have both the ability and incentive to favour their own related businesses (self-preferencing) at the expense of other business users of the platform."); CMA Online Platforms and Digital Advertising Market Study, *supra* note 94.

Self-preferencing itself is not prohibited by most competition laws,[394] which impose no general duty of dominant firms to assist their rivals.[395] However, antitrust agencies observe that self-preferencing conduct may violate abuse of dominance or monopolization prohibitions when the conduct involves above-listed (or other) forms of exclusionary conduct by a dominant firm such as monopoly leveraging or refusals to deal.[396] Self-preferencing is best understood as a specific variation on broader and more established theories of competitive foreclosure or exclusion.

The European Commission has several investigations into large digital platforms that exemplify these new theories of self-preferencing with anticompetitive effects.[397] For example, in addition to the Amazon matter mentioned above, the European Commission has now opened a second, more recent investigation into whether Amazon is foreclosing competition from its online marketplace through self-preferencing. The investigation will examine whether Amazon used its market power over Amazon Marketplace to prominently feature its own products over those of

[394] *But see,* recent amendments to German competition law create a new violation that would prohibit self-preferencing of a company's own services, where a company is found by the competition authority to "have paramount significance for competition across markets." Bundeskartellamt, Amendment of the German Act Against Restraints of Competition, at § 19(a) (Jan. 19, 2021), https://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2021/19_01_2021_GWB%20Novelle.html (abuse conduct by undertakings of paramount significance); *see also* French Autorité de la Concurrence & German Bundeskartellamt, Competition Law and Data Report, at 19 (May 10, 2016), https://www.bundeskartellamt.de/SharedDocs/Publikation/DE/Berichte/Big%20Data%20Papier.pdf;jsessionid=E302798FED37AC362CE2A36312543392.2_cid390?__blob=publicationFile&v=2 (describing "discriminatory access to data" as a potential abuse, provide it has a negative effect on competition, and discussing the Cegedim case where a medical information database provider refused to provide access to consumers who used competing software).

[395] *See, e.g.*, United States v. Colgate & Co., 250 U.S. 300, 307 (1919); Bruce Hoffman, Acting Dir. Bureau of Competition, FTC, Antitrust in the Financial Sector Remarks at Concurrences (May 2, 2018), https://www.ftc.gov/system/files/documents/public_statements/1408262/hoffman_-_antitrust_in_the_financial_sector_5-2-18.pdf (noting "[t]here is no general obligation under U.S. law to assist rivals.").

[396] *See, e.g.*, Crémer Report, *supra* note 110, at 66 (self preferencing does not violate Art. 102 of TFEU (abuse of dominance prohibition) unless it has anticompetitive effects or involves an essential facility); OECD, Abuse of Dominance in Digital Markets (2020) at 28-29, https://www.oecd.org/daf/competition/abuse-of-dominance-in-digital-markets-2020.pdf (recognizing that self-preferencing could involve refusals to deal, bundling, tying or margin squeezing); Crémer Report, *supra* note 110, at 66 (describing self-preferencing as a specific form of dominance leveraging); Singapore, Data: Engine for Growth *supra* note 14 at 78 (describing data-driven abuse that include discriminatory refusal to deal in data).

[397] *See, e.g.*, Eur. Comm'n Press Release IP/20/1073, Commission Opens Investigations into Apple's App Store Rule (June 16, 2020), https://ec.europa.eu/commission/presscorner/detail/en/ip_20_1073 (investigating whether Apple's app store rules imposed on app developers violate EU competition law, with a focus on e-book and music streaming rules); Eur. Comm'n Press Release IP/17/1784, Antitrust: Commission Sends Statement of Objections to Amazon for the Use of Non-Public Independent Seller Data and Opens Second Investigation into its E-Commerce Business Practices (Nov. 10, 2020), https://ec.europa.eu/commission/presscorner/detail/en/IP_17_1784 (fining Google for preferring its own shopping vertical search service in general Google search results).

third-party sellers who rely on the marketplace to compete with Amazon's own goods.[398] For example, the Commission is considering whether Amazon advantaged its own products in the criteria used to select the product featured in the prominently displayed "Buy Box" at the top of Amazon search results, which attracts consumer attention and purchases.[399] It will also look at whether Amazon gave preferential treatment to the subset of third-party sellers who use Amazon's logistics and delivery services.[400] In 2017, the Commission found violations by Google based on a similar theory of self-preferencing in search results.[401] Google was fined for preferring its own vertically integrated shopping-specific search service in the display of general Google search results.[402]

These self-preferencing theories have seen more attention, and even some enforcement success,[403] in jurisdictions like the EU, which imposes a heightened "special responsibility"[404] on dominant companies to ensure their conduct does not impede competition. Other jurisdictions, like Canada, have considered self-preferencing theories in digital platform enforcement investigations, but ultimately concluded that there was not a sufficient impact on competition arising from the conduct, and therefore no violation of antitrust law.[405]

[398] Eur. Comm'n Press Release IP/20/2077, *id.* (noting the opening of second investigation in Amazon over self-preferencing on its marketplace); Eur. Comm'n Press Release IP/20/1073, *id*. (investigating whether Apple's app store rules imposed on app developers violate EU competition law, with a focus on e-book and music streaming rules).

[399] Eur. Comm'n Amazon investigation, *id.*

[400] *Id.*

[401] Eur. Comm'n, Decision C (2017) 4444, Case AT.39740 – Google Search (Shopping) (July 27, 2017) (finding an abuse of dominance where Google preferred its own vertical properties in general search results, impacting competition).

[402] *Id.*

[403]Eur. Comm'n Press Release IP/17/1784, Antitrust: Commission Fines Google €2.42 Billion for Abusing Dominance as Search Engine by Giving Illegal Advantage to Own Comparison Shopping Service (June, 27 2017), https://ec.europa.eu/commission/presscorner/detail/en/IP_17_1784 (fining Google for preferring its own).

[404] Eur. Comm'n, Guidance on Its Enforcement Priorities in Applying Article 82 of the EC Treaty to Abusive Exclusionary Conduct by Dominant Undertakings, 2009/C 45/02, at ¶ 9 (2009) (noting special obligations on dominant undertakings); Crémer Report, *supra* note 110, at 70 (noting that dominant platforms "have a responsibility to ensure that they regulate in a pro-competitive way" in EU competition law).

[405] *See, e.g.*, Canada Competition Bureau Position Statement, Competition Bureau Statement Regarding Its Investigation into Alleged Anti-Competitive Conduct by Google (Apr. 19, 2016),

https://www.competitionbureau.gc.ca/eic/site/cb-bc.nsf/eng/04066.html (investigating whether Google's preferential treatment of its own vertical properties in search results violates competition law, but finding a lack of evidence of anticompetitive effects).

In jurisdictions such as the U.S., where dominant firms have no special obligations in antitrust law, federal antitrust enforcers have generally viewed such theories of self-preferencing with skepticism.[406] However, several U.S. state attorneys have brought claims that Google is engaging in competitive foreclosure, in a theory that relates to data privacy.[407] As mentioned above, Google has announced plans to block the access of third-party cookies from its Chrome internet browser. This would end the direct access to cookie data that advertisers and publishers currently rely on to compete with Google in online advertising.

The complaint alleges that this change is anticompetitive, because it "raise[s] barriers to entry and exclude[s] competition in the exchange and ad buying tool markets" by blocking cookies tracking by publishers and advertisers, who would otherwise compete with Google to deliver advertising.[408] The complaint claims that Google is "forcibly insert[ing] itself in the middle of publishers' business relationships," as advertisers and publishers who previously tracked users themselves will instead have to rely on Google as an intermediary once their cookies access is terminated.[409] This change, the states argue, will expand the already-dominant market power of Google's advertising businesses, contributing to its unlawful monopolization of ad buying and exchange markets. The complaint describes the company's asserted privacy justifications for the change as "a ruse" and mere "pretext."[410] Though best understood as a competitive foreclosure allegation, the claims can be described in some sense as Google "self-preferencing," because Google's own advertising tools will have access to tracking data that third parties will no longer be able to collect directly.

The U.K. competition authority has also expressed concerns over Google's plan to terminate third-party cookies access on Chrome, describing it as "a further example of platforms' increasing role in deciding on the appropriate application of data protection regulation for other market participants."[411] The agency has opened an investigation into whether Google's changes will have anticompetitive effects, but has not yet alleged any antitrust law violations.[412]

---

[406] *See, e.g.*, Bruce Hoffman, Acting Dir. Bureau of Competition, U.S. Fed. Trade Comm'n, Antitrust in the Financial Sector Remarks at Concurrences (May 2, 2018).

[407] Amended Complaint, Texas v. Google LLC, No. 4:20-cv-957-SDJ (E.D. Tex. March 15, 2021) at 96-99.

[408] *Id.* at 97.

[409] *Id.* at 98.

[410] *Id.* at 99 and 60.

[411] CMA Online Platforms and Digital Advertising Market Study, *supra* note 94, at ¶ 5.328. Cookies are a type of online tracking technology, often used in relation to online advertising.

[412] Press Release, CMA, CMA to investigate Google's 'Privacy Sandbox' Browser Changes (Jan. 8, 2021) (investigating Google's proposals to remove third-party cookies and other functionalities from its Chrome browser, including whether the proposed changes could cause advertising spend to become more concentrated on Google's ecosystem, reducing competition).

Google's policy change presents unique questions about whether and when practices that may improve privacy could also violate antitrust law. While many of the other topics in this Report suggest complementarity, or softer policy tensions at this intersection of law, the state enforcers' case (and other antitrust enforcement) against Google has the potential to materialize into a genuine conflict. Though it is early-stage, and there have not yet been any findings that either i) the conduct violates antitrust law or ii) that the alternative technology Google adopts will improve user privacy (privacy authorities are closely considering the privacy implications of Google's replacement ad technology), this Google policy change present an interesting dilemma in its potential for both.

This Google example reflects a more general policy concern, albeit not yet widely expressed, that dominant firms may self-preference their vertically integrated services in the interpretation of privacy obligations. The U.K. Furman Report on Digital Competition queries whether digital platforms' control over the sites of competition enables them to impose "unduly strict compliance duties on smaller firms, serving to reinforce their own dominance . . . .,"[413] essentially using data privacy law obligations as a tool for competitive exclusion. The U.K. CMA explains in a recent report that it is concerned large digital platforms:

> . . . have an incentive to interpret data protection regulations in a way that entrenches their own competitive advantage, including by denying third parties access to data that is necessary for targeting, attribution, verification and fee or price assessment while preserving their right to use this data within their walled gardens.[414]

Later in the same report, the CMA expresses more pointedly that:

> . . . our concern is that Google and Facebook have a clear incentive to apply a stricter interpretation of the requirements of data protection regulation when it comes to sharing data with third parties than for the use and sharing of data within their own ecosystems. . . . [T]his may even create an artificial incentive in the long run towards greater vertical integration.[415]

[413] Furman Unlocking Digital Competition, *supra* note 71, at 124-25.

[414] CMA Online Platforms and Digital Advertising Market Study, *supra* note 94, at 293.

[415] *Id.* at 296.

As described in the section on business justifications below, there are also numerous examples of large digital platforms announcing increases to privacy protective measures that are decried by their rivals for the resulting impact on competition.[416]

However, the research for this Report did not find any theories of privacy self-preferencing that had been established on the facts, or found to violate antitrust law. This type of competitive foreclosure is a very new potential interaction between antitrust and data privacy law. At this stage, it is best understood as part of the broader policy attention from both agency realms to the power and control exerted by large digital platforms over privacy and competition in the online ecosystem.

c. Novel Theories of Exploitative Abuse: Dominance and Meaningful Consumer Consent to Data Collection

In competition law, exploitative abuses involve a dominant entity extracting excessive or unfair rents. The classic example is exploitation of consumers through "excessive" pricing or margins.[417] While some jurisdictions recognize exploitative abuses of dominance,[418] others have almost no exploitative abuse cases.[419] Even in jurisdictions where exploitative abuses are recognized in theory, the vast majority of enforcement practice focuses instead on the exclusionary misconduct addressed in the prior section of this Report. However, exploitative abuses are addressed here for two reasons: i) there has been a recent uptick in attention to the

[416] *See* Part II.4.d. Data Privacy as a Justification for Alleged Anticompetitive Conduct.

[417] Exploitative theories of harm tend to focus on consumers rather than suppliers, but a notable recent exception to this is the German FCO's investigation into alleged exploitative abuses of third-party suppliers by Amazon. The case considered a wide variety of practices, from choice of law provisions in agreements, to policies and practices around ratings and notice of termination. The case, however, had no specific relevance to data privacy. Amazon settled the case by agreeing to change contractual and other business practices that impacted treatment of third-party sellers on its digital marketplace. Bundeskartellamt, Case Summary: Amazon Amends Its Terms of Business Worldwide for Sellers on Its Marketplaces – Bundeskartellamt Closes Abuse Proceedings (July 17, 2019), https://www.bundeskartellamt.de/SharedDocs/Entscheidung/EN/Fallberichte/Missbrauchsaufsicht/2019/B2-88-18.html;jsessionid=CBEBC85C2D4853BBE55E7DC0BD745795.2_cid387?nn=3600108.

[418] Eur. Comm'n, Communication from the Commission: Guidance on the Commission's Enforcement Priorities in Applying Art. 82 [now 102] of the EC Treaty to Abusive Exclusionary Conduct Abusive Exclusionary Conduct by Dominant Undertaking, Dominant Undertakings, 2009 O.J. (L 2009/C 45/02), at ¶ 7 (noting that exploitative conduct "is also liable to infringe" prohibitions on abuse of dominance), https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52009XC0224(01)&from=EN; *Act Against Restraints of Competition 2013* (GWB), §19(1) (2), nos. 2 and 3 (Ger.).

[419] U.S. antitrust law does not generally recognize exploitative abuses. *See, e.g.*, Phillip E. Areeda & Herbert Hovenkamp, Fundamentals of Antitrust Law § 16.06 (4th Edition, 2021-1 Supp. 2011) ("A monopolist does not violate Sherman Act §2 merely by restricting its output and charging an exploitative price.").

potential for exploitation of customers by dominant digital services,[420] and ii) one of the leading exploitative abuse cases emphasizes a unique interaction between the abuse and data privacy law. The coverage here is not meant to imply that exploitative abuse cases are widespread, or that they should be. The theories described may not be appropriate for adoption in the many countries where exploitative misconduct is rarely pursued by antitrust authorities.

Exploitative abuses have historically involved price. However, in a unique, recent case one antitrust agency has adapted the concept of exploitation to the context of data privacy. In 2016, the German Federal Cartel Office (FCO) commenced high-profile proceedings against Facebook for violating the exploitative abuse provisions of German competition law. As detailed in **Figure 6. Case Study: The German Federal Cartel Office Case Against Facebook**, below, the FCO alleges that Facebook used its market power in social networking services to impose terms of service on users that compelled "excessive" disclosure of personal data—beyond that which would have been granted in the absence of market power.[421] Specifically, the FCO claims Facebook had inadequate user consent for the collection and combination of users' data from Facebook's titular social networking service with two other sources: information from other Facebook services, such as Instagram and WhatsApp, and information from "off Facebook" (third-party) websites.[422] The FCO is concerned that Facebook conditions the use of its social network upon consent to the terms of service, which permit such data processing.[423]

The FCO claim against Facebook is unique because it casts a violation of privacy law as the anticompetitive act that then forms the basis for a violation in competition law. The argument is that the company's excessive data collection "is a manifestation of [its] market power," and therefore also an antitrust violation.[424] This unusual theory blends data privacy and antitrust law to a significantly greater degree than any other case to date.

[420] *See, e.g.,* Bundeskartellamt Amazon case, *supra* note 417, and the cases discussed in this section, *infra.*

[421] Press Release, Bundeskartellamt, Bundeskartellamt Prohibits Facebook from Combining User Data from Different Sources (Feb. 7, 2019), https://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2019/07_02_2019_Facebook.html.

[422] *Id.*; Bundeskartellamt Case Summary, Facebook Exploitative Business Terms Pursuant to Section 19(1) GWB for Inadequate Data Processing (Feb. 15, 2019), https://www.bundeskartellamt.de/SharedDocs/Entscheidung/EN/Fallberichte/Missbrauchsaufsicht/2019/B6-22-16.pdf?__blob=publicationFile&v=4.

[423] Bundeskartellamt Case Summary, *id.*

[424] *Id.* at 11.

Figure 6. Case Study: The German Federal Cartel Office Case Against Facebook

In 2016, the German Federal Cartel Office (FCO) began proceedings against Facebook alleging that the company violated exploitative abuse provisions in German competition law. The FCO argued that Facebook had used its market power in social networking services to impose terms of service on consumers that compelled "excessive" disclosure of personal data. In particular, the FCO is concerned that users consented to collection and combination of their Facebook data with information from i) other Facebook services, such as Instagram and WhatsApp, and ii) with data collected by Facebook about user activity that occurs on third-party sites ("off Facebook" data).[1] The FCO's view is that user consent to such collection was not sufficiently voluntary, because Facebook conditioned user access to Facebook services upon acceptance of the company's terms of service, "force[ing] its users to agree to the practically unrestricted collection and assigning of non-Facebook data to their Facebook user accounts." [1]

The FCO considers this conduct to be a privacy law violation, but does not have enforcement authority over privacy law. Instead, the FCO constructed a competition law violation around the conduct, arguing that the dominant position of Facebook, and the lack of other market options, impacted whether consent was freely given, and therefore its validity. The FCO argues that Facebook's ability to merge data sources was a result of, and substantially contributed to, its market power.[1] The agency imposed an initial remedy that prohibited Facebook from conditioning access to its service on consent to data collection and combination, and instead requiring that Facebook obtain "voluntary consent" from users for the practice of combining data.[1]

Facebook appealed the FCO's order to the Higher Regional Court in Düsseldorf. In August 2019, the appeal court suspended the FCO's initial decision pending further adjudication. It rejected the position that a dominant firm's violation of data protection law (if shown) would necessarily and automatically amount to a violation of abuse of dominance provisions. It concluded that users exercised autonomy in consenting to Facebook's terms and conditions of service, and that the data collection was not exploitative, as consumers were free to choose to make their data available to the same third parties through actions independent from Facebook. Overall, the appeal court found there was insufficient proof that Facebook's practices impaired competition.

The FCO appealed the Regional Court decision to the German Federal Court of Justice, which reinstated the order against Facebook in a June 23, 2020 decision. In determining whether an

abuse of dominance had occurred, the Federal Court found the decisive question was not whether there was a GDPR violation. Instead, it emphasized the FCO's view that the terms of service imposed by Facebook were abusive because they eliminated user choice regarding data processing, potentially impacting competition.

After further appeals, the case returned to the Higher Regional Court in Düsseldorf, which, on March 24, 2021 referred the case to the European Court of Justice. The referral includes questions about the FCO's jurisdiction to issue orders regarding violations of the GDPR, whether a possible GDPR infringement may be included in an assessment under antitrust law, and on the interpretation of effective consent and other justifications for data processing. The referral has the potential to result in a decision that lends insight into the relationship between antitrust and data privacy law from the perspective of EU law. The case is ongoing as of writing.

See:
Oberlandesgericht Düsseldorf [OLG Düsseldorf] [Düsseldorf Higher Regional Court] Mar. 24, 2021, VI-Kart 2/19 (V) (2021) (Ger.).

Bundesgerichtshof [BGH] [Federal Court of Justice] June 23, 2020, 23 Entscheidungen des Bundesgerichtshofes in Zivilsachen [BGHZ] KVR 69/19 (Ger.).

Oberlandesgericht Düsseldorf [OLG Düsseldorf] [Düsseldorf Higher Regional Court] Aug. 26, 2019, VI-Kart 1/19 (V) (2019) (Ger.).

Bundeskartellamt Case Summary, Facebook Exploitative Business Terms Pursuant to Section 19(1) GWB for Inadequate Data Processing (Feb. 15, 2019).

Bundeskartellamt Press Release, Bundeskartellamt Prohibits Facebook from Combining User Data from Different Sources (Feb. 7, 2019).

Other antitrust authorities have not followed suit with cases similar to that of the FCO.[425] However, the case has been followed with interest by both antitrust and data privacy authorities

[425] *But see* Press Release, Autorita Garante Della Concorrenza e del Mercato, Facebook 10 Million Euros by the ICA for Unfair Commercial Practices for Using Its Subscribers' Data for Commercial Purposes (Dec. 7, 2018). This case against Facebook was brought by the Italian Competition authority in 2018. Some of the violations appear to be consumer protection related, but others (as translated) seem to emphasize violations more akin to the FCO's exploitative abuses premised on data privacy violations. There is no mention of market power in the English

in policy reports and studies on the digital economy. Agencies have expressed at least two related, but more general, policy-level concerns around the adequacy of consent. First, agencies are considering the competitive and privacy effects of "take it or leave it" terms, where a service conditions access on consent to data collection. Second, though predominantly on the privacy side, agencies are considering the potential impact on privacy from data processing and aggregation that occurs across corporate families. The remainder of this section discusses these two issues.

i. Dominant Firms with "Take it or Leave it" Data Collection Terms of Service

Both antitrust and data privacy agencies have directed some attention to "take it or leave it," or binary consent terms of services, where the use of a service is conditioned on the consumer granting consent to data collection and processing. Some digital products and services require consent to data processing as a condition of access.[426] Others present consumers with options regarding use of their personal data, and still permit access to the product or service if a consumer refuses to allow some or all data processing. For example, many search engines allow consumers to opt-out of targeted advertising but still use searching functionality. In contrast, for many social media services, consumers must accept data collection and personalized advertising in order to access the service. Individuals are faced with the choice of either accepting the conditions of service or not using it at all. This conditioning of access to a service on data processing has been referred to variously as "take it or leave it" service offerings, "conditions of service,"[427] binary consent, or "bundling" of consent with acceptance of terms or conditions.[428]

Certain antitrust agencies view "take it or leave it" data processing terms as indicative of an imbalance in bargaining power between consumers and dominant digital platforms.[429] The

translation, but the "aggressive practices" are based on Facebook "exert[ing] undue influence" on users to automatically permit access to their data "without being able to make a free, informed choice." *Id*.

[426] CMA Online Platforms and Digital Advertising Market Study, *supra* note 94, at 13 (noting take it or leave it model of some platforms); Bundeskartellamt [FCO] Feb. 6, 2019, B6-22/16, *Facebook*, 2019 (Ger.).

[427] *See* Office of the Privacy Commissioner of Canada, Guidelines for Obtaining Meaningful Consent (May 2018), https://www.priv.gc.ca/en/privacy-topics/collecting-personal-information/consent/gl_omc_201805/ (explaining conditions of service as "[c]ollections, uses or disclosures of personal information over which the individual cannot assert any control (other than to not use a product or service)").

[428] GDPR, *supra* note 30, at Art. 7(4); ACCC Digital Platforms Inquiry Final Report, *supra* note 71 (using the term "bundled consent").

[429] ACCC Digital Platforms Inquiry Final Report, *supra* note 71 ("The ACCC also found considerable imbalance in bargaining power between digital platforms and consumers. Many digital platforms use standard for click-wrap agreements with take-it-or-leave-it term and bundled consents, which limit the ability of consumers to provide well-

concern is thought to be exacerbated where such terms are used by firms in concentrated markets, for services that consumers require, or at least will find it difficult to function without.[430] Such conduct could be cast as a consumer protection issue, but agencies such as the U.K.'s Competition and Markets Authority link it to competition as well, observing that:[431]

> [L]imited choice and competition also have the consequence that people are less able to control how their personal data is used and may effectively be faced with a 'take it or leave it' offer when it comes to signing up to a platform's terms and conditions. For many, this means they have to provide more personal data to platforms than they would like.

This echoes the FCO's case against Facebook, where few choices and "take it or leave it" terms of service allegedly led to disclosure of more data than would have occurred under competitive market conditions.

For data privacy agencies, "take it or leave it" terms raise questions about the impact of power imbalances on the legitimacy of data processing.[432] Where consent is the basis for lawful processing of data, the GDPR requires that consent be "freely" given with an "unambiguous indication of the data subject's agreement to the processing of personal data . . ."[433] The precise meaning of "freely" given remains the subject of interpretation, but European guidance indicates that there must be a genuine choice as to whether to accept or reject the terms.[434] Where there is an imbalance of power, including any element of "compulsion, pressure or inability to exercise free will," consent is not freely given, and thus not valid.[435] The result is that market power may impact whether consent is found to be freely given, and therefore affect the lawfulness of data

---

informed and freely given consent to digital platforms' collection, use and disclosure of their valuable data"). Note the ACCC specifically was not tasked with determining whether such terms constitute an abuse in the scope of the report, but rather finds such terms to be indicative of market power.; CMA Online Platforms and Digital Advertising Market Study, *supra* note 94, at 8.

[430] CMA Online Platforms and Digital Advertising Market Study, *supra* note 94, at 8.

[431] *Id.*

[432] GDPR prohibits processing of personal information except where permitted by law, and permitted basis include consent and the legitimate interests of the data processor (when certain conditions are met), among others. GDPR, *supra* note 28, at Art. 1(74); Crémer Report, *supra* note 110, at 80 (noting dominant firms may be subject to "a particularly stringent data protection standard" for both consent and legitimate processing grounds).

[433] GDPR, *supra* note 30, at Recital 32.

[434] Eur. Data Protection Board, Guidelines 05/2020 on consent under Regulation 2016/679 Version 1.1, at 5 (May 4, 2020), https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202005_consent_en.pdf.

[435] *Id.* at 7 (observing the role of imbalances of power in consent).

processing. The EDPS explains that:[436]

> In the case of 'free' online services, customers may not be offered an alternative version of a provider's offering in which personal information are not to be used for marketing purposes. Customers have limited room, if any, to negotiate the terms and conditions of use, representing a 'significant imbalance' between provider and user which could also trigger investigation into the legality of data processing. . . . Where there is a limited number of operators or when one operator is dominant, the concept of consent becomes more and more illusory.

Similar references to market power also appear in European guidance where data processing is based on the processor's own "legitimate interests," rather than consent. Under the GDPR, legitimate interests are a lawful basis for the processing of personal data, except where those interests are overridden by the interest or rights of the data subject.[437] EU guidance interprets market power as relevant to this balancing of interests in an assessment of whether there is a "legitimate interest."[438] Where a company holds a dominant position, the concern is that the firm may be able impose its views of a legitimate interest upon the data subject. This concern is exacerbated where consumers are presented with binary "take it or leave it" service offerings, rather than more fulsome consent optionality.[439]

These interpretations of consent and legitimate interests cast the GDPR in a role that parallels exploitative abuses of dominance in cases like the FCO's against Facebook. Both are considering how the misuse of market power could impact the rights or interests of a data subject in the processing of personal information. The perceived lack of optionality arising from a power imbalance between consumers and digital platforms appears in both the privacy and exploitative

[436] Preliminary Opinion of the EDPS, Privacy and Competitiveness in the Age of Big Data: the Interplay between Data Protection, Competition Law and Consumer Protection in the Digital Economy 35 (Mar. 2014).

[437] GDPR, *supra* note 30, at Art. 6(1)(f).

[438] Eur. Comm'n, Article 29 Working Party on the Notion of Legitimate Interests of the Data Controller Under Article 7 of Directive 95/46/EC, Opinion 06/2014 at 40 ("A large multinational company may, for instance, have more resources and negotiating power than the individual data subject, and therefore, may be in a better position to impose on the data subject what it believes is in its 'legitimate interest.' This may be even more so if the company has a dominant position on the market. If left unchecked, this may happen to the detriment of the individual data subjects. Just as consumer protection and competition laws help ensure that this power will not be misused, data protection law could also play an important role in ensuring that the rights and interests of the data subjects will not be unduly prejudiced."). Although this statement predates the GDPR, more recent guidance notes that existing Article 29 Working Party opinions on consent remain relevant where consistent with the new GDPR framework. European Data Protection Board, Guidelines 05/2020 on Consent Under Regulation 2016/679 Version 1.1, at ¶4 (May 4, 2020), https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202005_consent_en.pdf.

[439] EDPS Preliminary Op., Big Data 2014, *supra* note 436.

abuse contexts.[440] Giovanni Buttarelli of the European Data Protection Supervisor connects the potential privacy and competition implications as follows:[441]

> If a person has in effect only one choice of service provider in a digital market, then they are inevitably in a weak position to negotiate better quality of freedom of expression and privacy. If the service provider is dominant in the market, then it is potentially a competition issue, as well as a data protection and consumer issue.

Antitrust authorities in jurisdictions such as the U.S. are significantly more skeptical of such theories of informational exploitation. In emphasizing evidence-based approaches to antitrust, a former head of the DOJ Antitrust Division was critical of cases that "simply declare that data is the new digital currency, that online platforms have been exploiting data without consent, that loss of informational control is anticompetitive . . . ."[442] This reflects longstanding and deeply rooted differences in antitrust law across jurisdictions. While exploitative abuses are very rarely pursued in jurisdictions like the U.S., such theories are slightly more common in European jurisdictions (at least of late), as illustrated by the FCO's recent case.

ii. Use of Personal Data Across Corporate Families

Typically it is privacy authorities, rather than competition authorities, who are concerned with the adequacy of consumer consent to the collection and use of data across a corporate family. As discussed above, privacy agencies have taken action where, post-merger, data is used across corporate entities without adequate consent, in a manner may violate privacy law.[443] Privacy agencies have also taken enforcement action where no merger is involved, but data is being used across corporate entities without adequate consent. For example, the French data privacy authority (CNIL) fined Google for failing to obtain adequate consent across Google's plurality of

[440] *See, e.g.,* in the privacy context, Datasylnet (Norwegian Data Protection Authority), Big Data: Privacy Principles Under Pressure (2013) at 28 (discussing "imbalance" between companies and individuals, where enterprises that collect data are "extracting ever-increasing added value from the analysis and processing of [personal]… information" but individuals providing the information are not, making it more likely that transactions simply disadvantage individuals).

[441] EDPS, Giovanni Buttarelli, Opening Statement for Panel on Digital Rights and Enforcement, 10th Computers, Privacy and Data Protection Conference, at 2 (Jan. 26, 2017), https://edps.europa.eu/data-protection/our-work/publications/speeches-articles/26-january-2017_en.

[442] Makan Delrahim, Asst. Att'y Gen. Antitrust Div. U.S. Dept. of Just., Don't Stop Believin': Antitrust Enforcement in the Digital Era, Remarks as Prepared for Delivery at Booth School of Business, The University of Chicago, Chicago, IL (Apr. 19, 2018), https://www.justice.gov/opa/speech/assistant-attorney-general-makan-delrahim-delivers-keynote-address-university-chicagos.

[443] *See* Part II.3.a. Jurisdictional Limits and Post-Merger Enforcement Action (discussing action by privacy authorities after the merger of data-driven companies).

services, in violation of French data privacy law.[444] The CNIL explained that "[u]sers are not able to fully understand the extent of the processing operations carried out by Google. . . . [T]he processing operations are particularly massive and intrusive because of the number of services offered (about twenty), the amount and the nature of the data processed and combined."[445] Though dominance did not play an express role in the CNIL's findings, the agency mentions the "important place" that Google's Android operating system has in the French market, and the high number of Android users.[446]

Antitrust authorities are less concerned with the competitive effects of data sharing across related corporate entities. Antitrust enforcement typically involves conduct between unrelated corporate entities, such as mergers or unlawful agreements, rather than actions occurring within jointly controlled groups of corporations.[447] However, the FCO's case again provides a counter-example, because it alleges that Facebook's misconduct includes data sharing across its corporate family.

At a more general level, antitrust policy reports have considered whether a competitive advantage arises from the ability of large digital platforms to collect user data across multiple services within the company's digital ecosystem or footprint.[448] The Australian competition agency notes that such data conglomeration effects are likely to increase data barriers to entry for competitors in markets for online search and social networking.[449] This antitrust interest is not in

[444] National Data Protection Commission (Commission Nationale de l'Informatique et des Libertés) (Fr.), *The CNIL's Restricted Committee Imposes a Financial Penalty of 50 Million euros Against Google* (Jan. 21, 2019), https://www.cnil.fr/en/cnils-restricted-committee-imposes-financial-penalty-50-million-euros-against-google-llc ("users' consent is not sufficiently informed…. it is not possible to be aware of the plurality of services, websites and applications involved in these processing operations (Google search, You tube, Google home, Google maps, Playstore, Google pictures…) and therefore of the amount of data processed and combined."); *see* similarly, though brought under consumer protection law, *Austl Competition and Consumer Protection Comm'n v Google LLC* [2021] FCA 367 (16 April 2021) (alleging Google misled or deceived users of Google services when obtaining their consent to expand the scope of personally identifiable information collection and combination across Google services, third-party website and apps).

[445] *Id.* ("users' consent is not sufficiently informed. . . . it is not possible to be aware of the plurality of services, websites and applications involved in these processing operations (Google search, You tube, Google home, Google maps, Playstore, Google pictures . . .) and therefore of the amount of data processed and combined.").

[446] *Id.*

[447] *See, e.g., Copperweld Corp. v. Independence Tube Corp.*, 467 U.S. 752 (1984) (a wholly-owned subsidiary is incapable of conspiring with its parent company for the purposes of the cartel provisions of the Sherman Act).

[448] CMA Online Platforms and Digital Advertising Market Study, *supra* note 94, at Appendix F (noting that both Google and Facebook may have a competitive advantage arising from their ability to track users across their respective services, as well across third-party website and applications); ACCC Digital Platforms Inquiry Final Report, *supra* note 71, at 86 and 73-74 (reaching similar observations about Facebook and Google).

[449] ACCC Digital Platforms Inquiry Final Report, *supra* note 71, at 86 ("The ability of Facebook to merge off platform data with the unique data obtained via the user's interactions creates a very detailed picture of a user that

regard to the data sharing in and of itself, but rather the potential effects of such sharing on digital market competition.

Finally, the OECD briefly notes a variation on this theory in scholarly discussions, which posits that dominant firms might use their privacy policies as a means to leverage dominance from one market into another. The idea is that a dominant firm may engage in "privacy policy tying," where it imposes terms for data collection on consumers across several business units.[450] The theory posits that this could facilitate cross-service data sharing, enabling the firm to obtain the data necessary to leverage its dominance into an adjacent market with an overlapping need for data or user base.[451] Research for this report did not find other public consideration, much less uptake, of such a theory of privacy policy tying. It is not clear how such a theory would differentiate between beneficial cross-company data uses and those that harm consumers, which is an important distinction for the purposes of antitrust law.

d. Data Privacy as a Justification for Alleged Anticompetitive Conduct

Though rare and early-stage, antitrust cases and policy discussions have begun to raise the question of whether the protection of individuals' data privacy could justify otherwise anticompetitive conduct by a firm. This is one of the most nascent interactions on the horizon between the two areas of law.

Abuse of dominance is often subject to a "rule of reason" (effects-based) standard in antitrust law,[452] which means the conduct is analyzed using a burden-shifting framework. First, the plaintiff must establish a prima facie showing that the defendant's conduct has anticompetitive effects.[453] If shown, the burden then shifts to the defendant, who has an opportunity to prove that there is a pro-competitive, efficiency-based justification to explain its alleged misconduct. Such justifications typically involve proof that there is an economic benefit to consumers arising from

Facebook is able to track across not only on its own platform but on many other websites and apps. No other publisher or website, with the exception of Google, is likely to hold data that is as extensive as that collected by Facebook."); *id.* at 73-74 (expressing similar concern over Google's access to data from third-party sites, as well as across its own services, provides ad-targeting advantages).

[450] OECD, Abuse of Dominance in Digital Markets, at 55 (2020).

[451] *Id.*

[452] Most antitrust claims are evaluated under a rule of reason standard, which requires the plaintiff to plead and prove that anticompetitive effects arose from the impugned conduct. This is in contrast to the *per se* standard in antitrust law, under which anticompetitive effects are inferred from the nature of the conduct.

[453] *See* United States v. Microsoft Corp., 253 F.3d 34, 103 (D.C. Cir. 2001) (describing this burden-shifting framework).

the conduct. Provided the justification stands unrebutted by the plaintiff, or the procompetitive benefits of the conduct outweigh its anticompetitive effects, there is no antitrust law violation.

Companies facing claims of anticompetitive conduct are invoking the protection of their end-users' data privacy as such a justification. This creates a new facet of interaction between antitrust and data privacy law. Courts and enforcers have not yet determined whether data privacy protection could constitute a procompetitive justification in antitrust law.

However, the Canadian Competition Tribunal (Tribunal) had occasion to consider whether data privacy constituted such a business justification in a 2016 case against the Toronto Real Estate Board (TREB). The Tribunal is a specialized, adjudicative body that hears cases involving Canadian competition law. See **Figure 7. Case Study on User Data Privacy as a Justification for Anticompetitive Conduct: The Canadian Competition Tribunal and Toronto Real Estate Board**, below. The Canadian competition enforcement agency brought a claim against TREB that alleged the professional association had abused its dominance in residential real estate brokerage services. TREB had promulgated rules that denied online real estate brokers access to certain real estate listing data—data that TREB made available to traditional brick and mortar brokers. The online broker models posed a competitive threat to TREB's more traditional realtor members, undercutting their prices and providing more direct consumer access to real estate listings. In response to this claim of abuse of dominance, TREB argued that it had limited the online distribution of certain data, such as historical home selling prices, in order to protect the data privacy interests of the individuals who were selling their homes. TREB presented a number of arguments to support this position, including that its denial of online brokers access was necessary to comply with Canadian privacy law, and to comply with TREB's own terms and conditions of service for its home sales database.[454]

The Tribunal found that TREB's asserted privacy concerns were pretextual—an "afterthought," raised in the face of litigation, rather than a primary reason for TREB's exclusionary conduct.[455] There was no need to decide whether consumer privacy interests were in fact at stake, as the Tribunal found that on the facts, "privacy played a comparatively small role" in TREB's choice to adopt and enforce the disputed policy.[456] Instead, the evidence suggested that TREB's actions were driven primarily by the desire to limit competition from online realtors with TREB's more traditional realtor members, who charged higher prices.

[454] *See* Figure 7. Case Study: User Data Privacy as a Justification for Anticompetitive Conduct— The Canadian Competition Tribunal and the Toronto Real Estate Board.

[455] *Comm'r of Competition v. Toronto Real Estate Bd.*, 2016 Comp. Trib. 7 (Can.).

[456] *Id.*

Figure 7. Case Study: User Data Privacy as a Justification for Anticompetitive Conduct— The Canadian Competition Tribunal and the Toronto Real Estate Board

In 2011, the Competition Bureau Canada (Bureau) brought an abuse of dominance case against the Toronto Real Estate Board (TREB) in which TREB argued that consumer privacy justified its alleged anticompetitive conduct.

TREB is Canada's largest real estate board, and, at the time of the case, comprised nearly 50,000 real estate agents and brokers. The Bureau claimed that TREB had abused its dominant position in the market for residential real estate brokerage services in the Greater Toronto Area, by restricting new, online realtors from accessing, using and displaying certain data from its Multiple Listing Service Database (MLS). The database contained property listings and historical information about the sale of residential real estate.

While TREB allowed its members to share MLS sales data with clients by hand, email, or fax, consistent with traditional realtor models, it prohibited some of the same data from being provided to clients through new, online broker models. At the time of the case, there was no readily available substitute for the range of information and services provided on the MLS. The Bureau argued that TREB's data restrictions substantially prevented competition by limiting innovative, new online brokerage models, which were posing a competitive threat to TREB's traditional, offline members.

TREB argued that it had restricted its members online access and use of the disputed data because of concerns over the privacy of home-sellers.[457] TREB presented a collection of different arguments and evidence to suggest that individual sellers may not want particular home listing data online. TREB also claimed its rules were premised on an (unrelated) decision by the Office of the Privacy Commissioner of Canada, which found that an advertisement indicating the home selling price as a percentage of the listing price violated Canadian data privacy law. It argued that requiring consumers to consent to sharing their selling price data online as a condition of service would violate Canadian data privacy law. Finally, TREB asserted that the consent clauses in the agreements it recommended for use by member realtors only provided adequate consent for the disputed data to be disclosed in person, fax or email—not widely disseminated online.

In an April 27, 2016 decision, the Canadian Competition Tribunal (Tribunal) found that TREB's asserted privacy concerns were a pretextual "afterthought." There was no need to decide whether individuals' privacy interests were at stake, as the evidence indicated that

"privacy played a comparatively small role" in TREB's choice to adopt and enforce the disputed policy. Instead, TREB's decision was driven primarily by a desire to limit price competition from online brokers, who posed a competitive threat to the traditional, offline businesses of many TREB members. The Tribunal reasoned that TREB had provided the disputed data to third parties, and its traditional members, without significant privacy restrictions on further distribution—except the restrictions imposed upon the online realtor sites that were the subject of the case.

The Tribunal also looked at TREB's general practices around data and consumer consent, and found they bolstered the conclusion that the association's privacy argument was pretextual. TREB's policy was to refuse to allow individuals to delete their data on MLS, even when individuals expressly requested deletion. TREB instead took the position that listing data was essential to the operation of MLS and therefore could not be removed. In the face of other potential privacy concerns (unrelated those in the case), TREB had sought legal advice, and modified the consent provision in its standardized agreements in order to enable posting of interior home photos. However, there was no equivalent action reflected in the record for the alleged privacy concerns about the disputed selling price data. Finally, in other business contexts TREB had interpreted pre-existing consent to be sufficiently broad to allow the disclosure of consumer data, yet interpreted the consent requirements more narrowly in this case.

Despite finding that TREB had not established a privacy justification on the facts, the Tribunal recognized in *obiter dicta* that "there may be legal considerations, such as privacy laws, that legitimately justify an impugned practice, provided that the evidence supports that the impugned conduct was primarily motivated by such considerations." This suggests that data privacy protection could be recognized in competition law as a justification for anticompetitive conduct where it is the primary reason for such conduct.

Overall, the Tribunal found that TREB had abused its dominant position. TREB controlled the relevant market through its power over MLS, which was found to be a key input for the supply of residential real estate services. TREB had engaged in a practice of anticompetitive acts (which is required to violate Canadian abuse provisions) by passing and enforcing its rules that restricted access to certain MLS data for use and display online. The purpose of TREB's restrictions was to reduce competition between its members, by resisting the emergence of online brokerage models. The effect of the restrictions was to substantially reduce competition, eroding quality, innovation and variety in real estate brokerage services.

[457] TREB's privacy arguments were advanced among others, such as copyright, that are not described here.

TREB was ordered to remove its restrictions on data access and use for online real estate tools. TREB was unsuccessful in its efforts to appeal the Tribunal decision to both the Federal Court of Appeal and the Supreme Court of Canada.

See:
Comm'r of Competition v. Toronto Real Estate Bd., 2016 Comp. Trib. 7 (Can.). https://decisions.ct-tc.gc.ca/ct-tc/cdo/en/item/462979/index.do?q=toronto+real+estate+board+reasons.

Competition Bureau Canada, 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.

Though the research for this Report found no other agency cases considering whether data privacy may justify anticompetitive conduct, similar arguments have been raised in recent private (non-agency) litigation in the U.S. For example, LinkedIn, a professional social networking service, argued in a recent U.S. federal court case that user privacy concerns justified its alleged anticompetitive conduct. LinkedIn had blocked a data analytics company called HiQ from accessing user profiles on the LinkedIn social networking service.[458] HiQ claimed this was a violation of unfair competition law, engaged in to protect LinkedIn's competing services.[459] LinkedIn argued that HiQ was using individual profile data in a manner that violated the terms and conditions for the social media service, and user privacy.[460] In a preliminary decision, a California court found that the privacy rationale for the conduct did not appear substantiated on the facts.[461] The court issued a preliminary injunction that required LinkedIn to restore the rival's access to user data on the LinkedIn social media platform, and this remedy was upheld on appeal.[462]

[458] hiQ Labs, Inc. v. LinkedIn ,Corp., 938 F.3d 985 (9th Cir. 2019). HiQ was scraping information from users' LinkedIn profiles to feed its data analytics software, even where contrary to user privacy settings. When LinkedIn terminated its access to those profiles, HiQ brought several claims, including in state unfair competition law. The Though not an agency or federal law case, the decision is interesting because privacy is claimed as the justification for alleged anti-competitive conduct.

[459] *Id.*

[460] hiQ Labs, Inc. v. LinkedIn Corp., 273 F. Supp. 3d 1099, 1119 (N.D. Cal. 2017), aff 'd, 938 F.3d 985 (9th Cir. 2019).

[461] *Id.*

[462] hiQ Labs, Inc. v. LinkedIn ,Corp., 938 F.3d 985, 995 (9th Cir. 2019).

Digital platforms have also raised similar arguments in response to complaints lodged with antitrust authorities in the EU, and to Congressional inquiries in the U.S.[463] For example, Google and Apple have both been the subject of complaints to EU competition authorities in which rivals claim their apps were excluded from the digital giants' respective app stores in an anticompetitive manner.[464] The arguments are essentially that the companies are using their app store rules to exclude competing app distributors, in order to monopolize app distribution or particular types of app-based services.[465] In response, both companies have claimed that their actions were justified by the protection of user data security and privacy, and were not driven by anticompetitive animus.[466] Apple has also made these privacy and security arguments in defense of private litigation where it is accused of exclusionary app store conduct.[467] European competition authorities have reached a preliminary finding of abuse of dominance by Apple for

[463] H. Comm. on the Judiciary, Subcomm. on Antitrust, Commercial, and Admin. Law, 116th Cong., *Investigation of Competition in Digital Markets: Majority Staff Rep. and Recommendations*, at 55 (2020).

[464] Natalia Drozdiak, *Google Play Store Rival Files Antitrust Complaint to EU*, BLOOMBERG (July 12, 2018), https://www.bloomberg.com/news/articles/2018-07-12/google-play-store-rival-files-antitrust-complaint-to-eu(describing the second of two complaints by a rival app distributor against Google for exclusion from the Google app store); Tom Warren, *Apple Faces Another EU Antitrust Complaint As App Store Pressure Grows*, VERGE (June 16, 2020) (noting complaints against Apple made to European antitrust authorities by Rakuten, Spotify, and Tile, which make apps that compete with Apple); *see similarly* Complaint, SaurikIT LLC v Apple, 4:20-sv-08733 (N.D. Cal, Dec. 10, 2020) at 2-3 (noting the proliferation of monopolization allegations against Apple around the world related to control of the company's app store, and alleging Apple unlawfully maintained monopoly power in the markets for iOS app distribution, and iOS app payment processing).

[465] *See* sources cited at *id.*

[466] Dave Kleidermacher, *Android Security 2017 Year in Review*, Google Security Blog (Mar. 15, 2018), https://security.googleblog.com/2018/03/android-security-2017-year-in-review.html (Google taking the position that apps have been blocked and removed not to impede competition, but rather due to data privacy and security concerns); Adam Satariano, *Apple Defends App Store Policies After Spotify's Antitrust Complaint*, N.Y. TIMES (Mar. 15, 2019) (describing Apple invoking consumer interests in the "App Store [being] a safe, secure platform" in response to Spotify's allegations of anti-competitive conduct).

[467] Epic Games, Inc. v. Apple Inc., 20-cv-05640-YGR (N.D. Cal. 2020). In this ongoing, high-profile case, Apple is accused of maintaining an unlawful monopoly over the distribution of apps for Apple devices. Apple is also accused of engaging in tying, by requiring the mandatory use of Apple's in-app payment services (from which Apple earns a percentage fee) as a condition of distributing certain apps through the Apple app store. Apple's response has included arguments that user data privacy and security concerns justify the rules it imposes on third-party apps as a condition of their access to the Apple app store.

its app store practices,[468] and the U.K. competition authority is conducting an ongoing investigation into Apple for similar conduct.[469]

It is not yet clear which, if any, of these allegations will proceed, and whether any amount to anticompetitive conduct in antitrust law. Competition law does not generally impose a duty to deal with competitors, so the claims would have to establish that the exclusion of particular rivals also had an effect on overall competition. Still, the arguments hints at what is to come between antitrust and data privacy, where allegations of anticompetitive conduct are met with a response that the action was justified in the name of user data privacy protection.

Antitrust and data privacy agencies have also recognized a related policy concern—that dominant digital platforms may have the power and ability to over-interpret the privacy obligations they impose on other market participants, as a means to exclude competitors and entrench their own market power.[470] This worry is discussed in the section above, on theories of competitive foreclosure or self-preferencing of large platforms' own vertically integrated services.[471] In the face of antitrust scrutiny of its over-interpretation, the platform might then invoke user data privacy protection as a cover for anticompetitive conduct. The EDPS explains this concern:[472]

> A dominant undertaking could thus seek to justify its refusal to supply competitors with datasets, including through exclusivity agreements, by claiming to adhere to data protection rules. Such refusal to supply, it has been argued, may have an anticompetitive effect: if there are limits on disclosure of datasets to competitors, the dominant undertaking could prevent the development of competing products from competitors. The undertaking could, therefore,

[468] Eur. Comm'n Press Release IP/21/2061, Antitrust: Commission Sends Statement of Objections to Apple on App Store Rules for Music Streaming Providers (Apr. 30, 2021), https://ec.europa.eu/commission/presscorner/detail/en/ip_21_2061 (announcing preliminary finding that Apple's rules for the distribution of third-party apps via its App Store, and related conduct, violate EU competition law). Apple is reportedly also under investigation in the U.S. for its app store practices. Leah Nylen, *Apple's Easy Ride from U.S. Authorities May Be Over*, POLITICO (June 24, 2020), https://www.politico.com/news/2020/06/24/justice-department-anti-trust-apple-337120.

[469] Press Release, CMA, CMA Investigates Apple Over Suspected Anti-Competitive Behaviour (Mar. 4, 2021) (investigating whether Apple used its dominance to impose unfair or anti-competitive terms on developers who use the company's App Store, resulting in less choice or higher prices for apps).

[470] CMA Online Platforms and Digital Advertising Market Study, *supra* note 94, at 293 ("Our concern is that such platforms have an incentive to interpret data protection regulation in a way that entrenches their own competitive advantage, including by denying third parties access to data that is necessary for targeting, attribution, verification and fee or price assessment while preserving their right to use this data within their walled gardens.").

[471] *See* Part II.4.c.i. Dominant Firms with "Take it or Leave it" Data Collection Terms of Service.

[472] EDPS Preliminary Op., Big Data 2014, *supra* note 338 at 31 (footnotes omitted).

try to 'shield' itself from remedies potentially imposed by competition authorities by claiming compliance with data protection rules.

Claims of data privacy as a business justification present an opportunity for productive collaboration between antitrust and data privacy authorities. The expertise of data privacy authorities could provide insight to antitrust authorities in their factual determination of whether privacy protection or interests are truly at stake, and to ensure an accurate understanding of the scope of protected privacy interests. If the facts indicate that privacy protection was the primary reason for the defendant's conduct—unlike in the TREB case—then antitrust enforcers and courts will also face the legal question of whether data privacy constitutes a procompetitive business justification.

This section considers recent cases and complaints where dominant firms claim the protection of data privacy as a justification for their allegedly anticompetitive conduct. Though discussed in the context of abuse of dominance here, it is worth noting that similar questions of whether privacy is a business justification could arise for any type of conduct subject to the rule of reason burden-shifting framework described at the outset of this section. This includes, for example, certain types of agreements between competitors. So far the issue has been raised only in the abuse of dominance context—as next section of this Report describes, privacy has not been an issue in such other types of misconduct.

5. Data Privacy Considerations in Cartels and Competitor Collaborations

Cartel laws around the world prevent agreements between competitors to fix prices, allocate markets or restrict output. Such unlawful collusion is often viewed as the most egregious type of antitrust violation, and tends to be prohibited under criminal rather than civil competition law.

To date, there has been little to no agency discussion of the relationship between cartels and data privacy. Cartels are discussed briefly here for completeness, as cartel enforcement is a robust and important part of antitrust law. The primary area of shared attention from antitrust and data privacy authorities is the broader issue of transparency of algorithmic decision-making.

The OECD has raised the hypothetical potential for a cartel between zero-price product suppliers that aims to set or reduce data privacy or protection safeguards,[473] but provides no examples where such conduct has occurred. As antitrust analysis is typically price-based, determining the effects on competition of a cartel on privacy quality, rather than price, would likely present analytical challenges that echo those discussed above.

[473] OECD, Zero-Price Markets – Background Note, *supra* note 9, at 14.

a. Algorithmic Transparency and Collusion

Algorithms are "sequences of instructions to perform a computation or solve a problem."[474] Algorithmic processes are not new, but the use of algorithms has increased in ubiquity, complexity and power with the proliferation of digital data and artificial intelligence. This has drawn the attention of both antitrust[475] and data privacy[476] authorities to the role of algorithms in digital commerce and privacy, respectively. The main shared interest is that of transparency and trust in algorithmic decision-making, which is discussed above, along with other common policy interests of both regimes.[477] Beyond that, the impact of algorithms and related questions around artificial intelligence are of interest to both policy spheres, but for reasons that appear to be distinct in each realm.

The primary concern of antitrust agencies, and the subject of numerous policy reports, is the potential role of algorithms in facilitating unlawful collusion between competitors, or to otherwise reduce competition.[478] The use of algorithms is neither inherently harmful nor inherently beneficial to competition. However, along with the rise of big data, there has been a proliferation of algorithm-driven business models and decision-making processes across many areas of the economy. This new ubiquity has raised questions about the potential for algorithmic pricing to facilitate collusion, by making detection and response to cartel "cheating" easier to detect (where one member of the cartel deviates from the anticompetitive agreement). Violations of cartel provisions may also occur where firms agree to use the same algorithm to set prices,

[474] CMA Algorithms Report, *supra* note 94.

[475] *Id.*; Competition Bureau Canada Big Data Report *supra* note 68, at 9-10 (discussing the potential role of algorithms in cartel conduct); Singapore, Data: Engine for Growth *supra* note 14, at 66-67 (discussing algorithmic collusion); OECD, Algorithms and Collusion: Competition Policy in the Digital Age, https://www.oecd.org/daf/competition/Algorithms-and-colllusion-competition-policy-in-the-digital-age.pdf.

[476] *See, e.g.*, U.K., ICO, Big Data, Artificial Intelligence, Machine Learning and Data Protection, at 86-89, https://ico.org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf (discussing algorithmic transparency); EDPS, Opinion 7/2015 Meeting the Challenges of Big Data, at 8 https://edps.europa.eu/sites/default/files/publication/15-11-19_big_data_en.pdfhttps://edps.europa.eu/sites/default/files/publication/15-11-19_big_data_en.pdf (noting impacts of lack of transparency).

[477] *See* Part I.4.a. Promoting Trust in Digital Markets.

[478] CMA Algorithms Report, *supra* note 94 at 20 (noting extensive global competition scholar and agency attention to algorithmic collusion theory); German Bundeskartellamt & Autorité de la Concurrence, Algorithms and Competition (Nov. 2019); Competition Bureau Canada Big Data Report *supra* note 68, at 9 (noting that a "prominent question" in competition law has been the role of algorithms).

either by traditional agreement,[479] or by delegating pricing decisions to a shared intermediary who uses algorithms to co-ordinate the unlawful price fixing.[480] There has also been some suggestion that algorithms may self-learn to collude, reducing competition.[481] Though such tacit collusion may impact competition, in the absence of an express or implied agreement the conduct is unlikely to be prohibited by antitrust law.

Antitrust agencies have also expressed concern that algorithms could contribute to the exclusion of competitors in digital markets, by enabling platforms to give preferential treatment to their own products or services.[482] This concern is not specific to algorithms, but rather reflects broader concerns over online gatekeeping and self-preferencing, which are discussed above.[483]

6. Data Privacy and Antitrust Remedies

Once an antitrust law violation is found, courts will impose remedies to restore or maintain competition. Or, where antitrust authorities allege a violation, the accused firm may also reach a negotiated settlement agreement to resolve the alleged effects on competition. These remedies may implicate data privacy in a manner different from the misconduct itself. Although this interaction is at a very early stage, this section describes the potential data privacy implications of antitrust remedies that compel access to personal data or interoperability.

Antitrust remedies aim to promote competition, either by ending the anticompetitive conduct and restoring competition in cases of abuse or cartels, or by preventing the anticompetitive effects

[479] Press Release, U.S. Dep't of Justice, *Former E-Commerce Executive Charged with Price Fixing in the Antitrust Division's First Online Marketplace Prosecution* (Apr. 6, 2015), https://www.justice.gov/opa/pr/former-e-commerce-executive-charged-price-fixing-antitrust-divisions-first-online-marketplace; Plea Agreement, United States v. Topkins, No. 3:15-cr-00201-WHO (N.D. Cal. Apr. 30, 2015); Press Release, CMA, *Online Seller Admits Breaking Competition Law* (July 21, 2016), https://www.gov.uk/government/news/online-seller-admits-breaking-competition-law.

[480] CMA Algorithms Report, *supra* note 94, discussion at footnote 109 (addressing the potential for algorithmic collusion through a shared intermediary).

[481] *See, e.g.*, *id.* at 19 (enumerating categories of algorithmic collusion theory).

[482] *Id.* at 16 (discussing self-preferencing in algorithms by Google and Amazon); Eur. Comm'n Press Release, Antitrust: Commission Sends Statement of Objections to Amazon for the Use of Non-Public Independent Seller Data and Opens Second Investigation into its E-Commerce Business Practices (Nov. 10, 2020), https://ec.europa.eu/commission/presscorner/detail/en/ip_20_2077; Eur. Comm'n, Decision C(2017) 4444, Case AT.39740 – Google Search (Shopping) (July 27, 2017).

[483] *See* Part II.4. Data Privacy Considerations in Abuse of Dominance/Monopolization Analysis.

likely to be caused by mergers.[484] Discussion of antitrust remedies is commonly bifurcated into "behavioral" or conduct remedies, and "structural" remedies, though both may be imposed in the same matter.[485] A structural remedy involves divestiture or dissolution of the defendant into separate entities. A behavioral remedy seeks to control the conduct of the defendant, by preventing or requiring certain action (or both). Behavioral remedies are much more common in antitrust cases, and, so far, have received more attention for their potential data privacy implications. Structural remedies may also give rise to impacts on data privacy, but those are as-yet largely unexplored in publicly available agency materials.

Where a merger or misconduct is found to violate antitrust law, antitrust behavioral remedies may require the defendant to provide rivals with access to data or to ensure interoperability, as a means of restoring (or maintaining, for mergers) competition. These types of remedies—compelled access to, or disclosure of, information, or mandated interoperability—appear to have the greatest potential to implicate data privacy, particularly where personal data is involved.[486]

It is important to note that antitrust law uses such compelled data access and interoperability remedies sparingly, and with restraint.[487] The concern is that, if used too widely, compelled data access could undermine the incentives of data-driven firms to provide innovative products and services to the benefit of consumers.[488] There is no general obligation in antitrust law to disclose or share competitively important data.

However, the topic of such remedies has taken on new prominence in the digital policy context. Discussions about digital platform enforcement or regulation often include consideration of the

[484] *See, e.g.*, United States v. Microsoft Corp., 253 F.3d 34, 103 (D.C. Cir. 2001) (describing antitrust remedial goals as ending the anti-competitive conduct, ending the illegal monopoly, ensuring that there remain no practices likely to result in monopolization in the future and denying the defendant the fruits of its violation).

[485] *See, e.g.*, U.S. Dept. of Justice, Single-Firm Conduct Guidelines, at 149 (Sept. 2008), (https://www.justice.gov/sites/default/files/atr/legacy/2009/05/11/236681.pdf (discussing structural vs. conduct remedies).

[486] *See, e.g.*, U.K. Info. Comm'r Off. & CMA, Competition and Data Protection in Digital Markets: A Joint Statement Between the CMA and the ICO (May 19, 2021) at 23-24 (observing the potential for data privacy and competition objectives to be in tension where "data related interventions that seek to overcome barriers to competition by providing third-parties with access to personal data," but noting that such tension "can be resolved" through careful remedy design).

[487] *See, e.g.*, Personal Data Protection Comm'n of Singapore & Competition and Consumer Comm'n of Singapore, Discussion Paper on Data Portability ¶ 3.30 (Feb. 25, 2019) ("it is only in very limited circumstances that competition law enforcement will achieve an outcome where an organisation is required to share its data.").

[488] *See, e.g.,* Furman Unlocking Digital Competition, *supra* note 96, at 74 ¶ 2.87-88 (noting data access is "more interventionist" than other remedies considered, and the importance of assessing the impact of mandated access on incentives for future investment in future data collection and management).

potential for remedies that compel interoperability with, or access to, the data held by these platforms.[489] For antitrust, this remedies emphasis is a corollary to theories of harm that focus on the competitive value of data, and the effects of foreclosing rivals from data access.[490] For example, the head of the EU competition authority warns that "as data becomes increasingly important for competition, it may not be long before the Commission has to tackle cases where giving access to data is the best way to restore competition."[491] Similarly, a 2019 U.K. report on digital competition observes that "in some markets, the key to effective competition may be to grant potential competitors access to privately-held data."[492] The same report acknowledges, however, that any such mandated data sharing would also need to comply with the privacy rights and expectations of the individual data subjects, and that the GDPR may prevent such personal data processing, unless the data is aggregated or anonymized.[493]

Jurisdictions like the U.S., however, have generally been more reticent in considering mandated access to competitively important resources. A former head of the U.S. DOJ Antitrust Division observes:[494]

> Recognizing the benefits of data, some commentators have argued in favor of requiring dominant firms to share data with smaller competitors. They argue that a refusal to share data by a dominant platform is anticompetitive. In the United States, however, we do not generally require firms, even dominant ones, to deal with competitors. I am not yet convinced that we should have different rules for data.

The FTC appears slightly more open to the potential data access remedies in cases involving mergers rather than abuse. An FTC Director of the Bureau of Competition observes: "[t]he breadth of additional relief [in merger review] that may be considered include obligations to

[489] *Id*. at 68-69 (suggesting an *ex ante* regulatory regime that could regulate digital platforms by mandating interoperability and third-party access to data "where data is valuable in overcoming barriers to entry and expansion and privacy concerns can be effectively managed").

[490] *See* Part II.4. Data Privacy Considerations in Abuse of Dominance/Monopolization Analysis.

[491] Margrethe Vestager, Comm'r of Competition, Eur. Comm'n, Defending Competition in a Digitised World, Address at the European Consumer and Competition Day (Apr. 4, 2019), https://wayback.archive-it.org/12090/20191129202059/https://ec.europa.eu/commission/commissioners/2014-2019/vestager/announcements/defending-competition-digitised-world_en; Crémer Report, *supra* note 110, at 99 (opining that where there are significant foreclosure effects on competition arising from a denial of data access "the need to ensure the possibility of entry may argue in favour of mandating access to data.").

[492] Furman Unlocking Digital Competition, *supra* note 96, at 74 ¶ 2.81-82.

[493] *Id.*

[494] Makan Delrahim, Asst. Att'y Gen., Dept. of Justice, *"Start Me Up": Start-Up Nations, Innovation, and Antitrust Policy*, (Oct. 17, 2018).

provide inputs, distribution, access or other rights, data, or supply of products and services to one or more entrants on specified terms or a non-discriminatory basis for some period of time."[495]

Past antitrust cases with mandated data access or interoperability remedies have tended to involve disclosure of non-personal data, such as business plans or interoperability information.[496] Even for those older cases that did involve disclosure of personal data, data privacy law simply did not have the same relevance in the past as it does now, and it was not considered.[497] Remedies in cases today have a greater potential to implicate personal data and data privacy law in the antitrust remedies.[498] This is particularly true for remedies against firms in those digital markets where the monetization of personal data plays an important role in competition. When a modern antitrust remedy mandates that the defendant grant access to personal data, individual privacy interests and rights of data subjects are likely to be a relevant consideration.

Though relatively rare to date, there are a few examples of litigated and settled cases where data privacy has been expressly considered in the design of the antitrust remedies. First, remedies have been designed to accommodate data privacy interests, by permitting the individuals whose data is at stake to opt-out of disclosure. When such opt-out occurs, the defendant is relieved of its remedial obligation to grant access to the personal data that it holds. U.S. antitrust authorities took this opt-out approach in a 2005 case against a real estate broker association.[499] The remedy required that the defendant association disclose residential real estate listing data to realtors for distribution online—including detailed information about individuals' homes that were for sale. Consumers who did not want data about their home distributed online could opt-out of having their home listing data disclosed for such purposes, or could choose to withhold certain data from online listings, like an estimate of their home's market value.[500] Under the remedy, the defendant

[495] Ian Conner, Dir., Fed. Trade Comm'n, Remarks at GCR Live 9th Annual Antitrust Law Leaders Forum (Feb. 8, 2020), https://www.ftc.gov/system/files/documents/public_statements/1565915/conner_gcr_live_conduct_remedies_2-8-20.pdf (emphasis added).

[496] *See, e.g.*, Erika M. Douglas, *Monopolization Remedies and Data Privacy*, 24 VIR. J. L. & TECH. 2, 33-67 (2020) (discussing the distinctions between past data access remedies and those likely in the digital economy).

[497] *Id.*; *see, e.g.*, Eur. Comm'n, Case No COMP/M.4726 – Thomson Corporation/ Reuters Group (mandating disclosure of a database that included personal information); Great Western Directories, Inc. v. Southwestern Bell Telephone Co., 63 F.3d 1378 (1995) *withdrawn and superseded in part,* 74 F.3d 613 (5th Cir. 1996), *vacated pursuant to settlement* (Aug. 21, 1996) (requiring disclosure of consumer phone listing data).

[498] Douglas, *supra* note 496, at 47-67.

[499] United States v. Nat'l Ass'n of Realtors, 2008 WL 5411637, at *13 (N.D. Ill. Nov. 18, 2008) (Section 1 Sherman Act claim challenging the association's member policy, which denied online realtors the same access to listings of homes for sale provided to traditional realtors, reducing competition).

[500] *Id.* at Exhibit A, ¶ II.5 and Appendix A (seller opt-out form).

was not required to disclose the personal data of the consumers who opted-out.[501]

Similarly, the French competition authority used an opt-out approach in an interim remedy imposed on a dominant gas supply company. The company was required to provide rivals with information about its gas customers, such as individual's names, addresses, telephone numbers and consumption profiles.[502] The French data protection authority was consulted in the design of the remedy. The end result enabled individuals to opt-out, and upon doing so, their information was excluded from the mandated data-sharing by the defendant.[503]

In both this French gas supply case and the U.S. realtor case above, the remedies were designed used opt-out mechanism. However, as data privacy law moves toward increasingly robust conceptions of consent—for example, preferring opt-in rather than the opt-out models, and greater optionality in the specifics of consent—antitrust authorities may be harder-pressed to craft effective and administrable remedies centered around consent.[504]

Further, these cases involved episodic or one-off transfers of data. Remedies that require ongoing interoperability to enable a flow of personal data may raise even more pressing questions about data privacy. In past cases, antitrust authorities have imposed obligations aimed at ensuring interoperability with the products of dominant or merging firms, most notably in cases that involve computer software.[505] Particularly in digital markets, interoperability continues to be part of the dialogue around potential antitrust remedies.

It is not yet clear how modern data access or interoperability remedies will account for data privacy. However, as the UK competition and data privacy authorities observed in a joint report,

---

[501] *Id.*

[502] French Autorité de la Concurrence, Décision n° 14-MC-02, Relative à une Demande De Mesures Conservatoires Présentée par la Société Direct Energie Dans Les Secteurs du Gaz et de L'électricité (Sept. 9, 2014), https://www.autoritedelaconcurrence.fr/sites/default/files/commitments//14mc02.pdf. The case was the subject of a number of appeals, and, ultimately, a settlement agreement was reached that imposed a fine on GDF Suez (which became Engie) for abuse of dominance. Press Release, French Autorité de la Concurrence, L'Autorité de la Concurrence Sanctionne ENGIE Pour Avoir Abusé de sa Position Dominante (Mar. 22, 2017), https://www.autoritedelaconcurrence.fr/fr/communiques-de-presse/lautorite-de-la-concurrence-sanctionne-engie-pour-avoir-abuse-de-sa-position.

[503] *Id.*

[504] For further discussion of the challenges of a consent model for antitrust remedies that mandate disclosure of personal data, *see* Erika M. Douglas, *Monopolization Remedies and Data Privacy*, 24 VIR. J. L. & TECH. 2, at 79-84 (2020).

[505] *See, e.g.*, *Microsoft*, 253 F.3d. at 99-100; Case T-201/04, Microsoft Corp. v. Comm'n, 2007 E.C.R. II-3601 (affirming a remedy requiring Microsoft to share interoperability information).

it is clear that "where access to personal data is in scope [for] such a remedy, it must be designed in a way that aligns with data protection law."[506]

Second, merger remedies have been imposed where one or both of the parties holds sets of personal data that reinforce or reiterate the parties' data privacy law obligations. Such remedies were recommended by the Colombian competition authority in its review of a joint venture involving the three largest Colombian banks. The Colombian authority is somewhat unique in that, like the FTC, it enforces three areas of law—competition, consumer protection and privacy. This bank joint venture, discussed in detail in **Figure 8. Case Study—Colombia Digital Identity Joint Venture**, below, proposed to offer the first digital identity verification service for financial services in Colombia. The Colombian competition authority recommended that, as part of the conditions of permitting the joint venture, participants be required to comply with data protection law.[507] Though already subject to data protection law, this would reinforce the existing obligation through an antitrust remedy. Much like the realtor and gas-supply cases discussed above, the remedy also included an obligation to obtain express and informed consent from bank clients before migrating their personal data from the individual banks to the joint venture.

[506] U.K. Info. Comm'r Off. & CMA, Competition and Data Protection in Digital Markets: A Joint Statement Between the CMA and the ICO (May 19, 2021) at 23.

[507] In this case, the Colombian competition authority reviewed the proposed joint venture, then made recommendations to the financial regulatory authority that it impose the described limitations on the joint venture, and on the participating banks.

Figure 8. Case Study: A Colombian Digital Identity Joint Venture

In 2019, the Colombian competition authority reviewed a joint venture between the three largest Colombian banks. The banks held approximately 60% of the financial services market by income. The joint venture planned to provide digital identification services for the authentication of financial services customers. This innovative new digital identification verification offering was the first of its kind in Colombia, and once established, would comprise 100% of the relevant market. The joint venture's digital identity services were expected to bring banking customers more flexible and convenience in accessing financial services, increased privacy, security and control over their financial information, and to promote inclusion in financial services across the Colombian population. For the banks, the joint venture promised to reduce the risks of fraud, by making reliable and up-to-date data on consumers available for bank decision making and, as a result, was also expected to lower operating costs.

Upon completing its review, the Colombian competition authority recommended to the Colombian financial supervisory authority that it impose several conditions on the joint venture. The suggested conditions included, among other obligations:

- A requirement that the joint venture comply with data protection law;
- A requirement that the joint venture obtain express and informed consent from individual banking clients before migrating their personal data from the banks over to the joint entity; and
- Interoperability requirements for the joint venture's platform, to ensure future entrants could access the client banking data necessary to compete to offer other digital identification verification services. Given the joint venture was the only one of its kind, and involved all three of the largest banks in Columbia, this data access obligation was intended to address competition authority concerns over barriers to entry for future competition in digital identity verification services.

See:
Industry y Commercio Superintendencia, Referencia Respuesta a Solicitud de Análisis de Una Operación de Integración Epresarial Entre Bancocolombia S.A, Banco Davivienda S. A. y Banco de Bogota S.A (translation), July 29, 2019, https://www.sic.gov.co/sites/default/files/files/integracion_empresarial/pdf/2019/julio/BANCOLOMBIA%20-%20DAVIVIENDA%20-%20BANCO%20DE%20BOGOT%c3%81.pdf.

The European Commission imposed similar privacy law compliance conditions on Google's acquisition of Fitbit, a health and fitness company.[508] The competition remedy, designed in consultation with the EDPS, required that Google provide European Economic Area users with "an effective choice to grant or deny the use of health and wellness data stored in their Google Account or Fitbit Account by other Google services," like Google Search, Maps or YouTube.[509] This was despite the Commission's acknowledgement that Google would already be obligated to ensure compliance with the GDPR, and that personal data processing concerns raised by the merger were "not within the remit of merger control."[510] The merger review was conducted in cooperation with the European data privacy authority (EDPS), and the commitments were negotiated with the merging parties, both of which may explain the appearance of this data protection obligation even in the absence of any finding of impacts on privacy-based competition.[511]

On the privacy agency side, EDPS similarly describes the potential for antitrust remedies to advance privacy interests, such as by requiring data portability, or by restricting information processing across the different corporate entities of a business.[512] These comments, and the privacy-law bolstering remedies seen in *Google/FitBit* and the Colombian banking joint venture, are a somewhat awkward fit with the position that has been articulated in U.S. and EU in merger reviews that the agencies lack the jurisdiction to consider any merger effects on privacy that are unrelated to competition.[513] This jurisdictional question was effectively bypassed by *Google/Fitbit* remedy, because (as is often the case in merger reviews) the remedy took the form of voluntary commitments negotiated between the merging parties and the reviewing agency, rather than litigated remedies. Since the commitments were voluntary, the parties were free to add any agreed-upon terms, including the privacy-related obligations.

Finally, antitrust authorities have imposed merger remedies that sequester or silo the data held by merging parties, in order to limit the anticipated effects on competition arising from the combination of data. Where the combination of certain data is expected to lead to anticompetitive

[508] Eur. Comm'n Press Release IP/20/2484, Mergers: Commission Clears Acquisition of Fitbit by Google, Subject to Conditions (Dec. 17, 2020), https://ec.europa.eu/commission/presscorner/detail/en/ip_20_2484.

[509] *Id.*

[510] *Id.*

[511] *Id.*

[512] EDPS, Privacy and Competitiveness in the Age of Big Data: The Interplay Between Data Protection, Competition Law and Consumer Protection in the Digital Economy, at 34-35 (Mar. 2014), https://edps.europa.eu/sites/edp/files/publication/14-03-26_competitition_law_big_data_en.pdf.

[513] *See* Part II. 3. Data Privacy Considerations in Merger Review (discussing this agency view on jurisdictional limits).

effects, the merging parties and antitrust authorities have reached agreements to maintain the data separately post-merger, as a condition of merger approval.[514] The European Commission's remedies in Google/Fitbit offers an example of this type of obligation as well. The agency considered the impact of Google combining its vast amounts of ad data with Fitbit's information about users' health and fitness, and its likely impact on competition. As a condition of receiving merger approval, the Commission required Google to maintain a technological "data silo" that stores FitBit user health and fitness data separately from the data that Google uses for online advertising.[515] The purpose of this data separation obligation is to limit anti-competitive effects. However, since the silo covers some data that is personal, and also sensitive health data, the antitrust obligation may also have incidental benefits for privacy, by preventing such data from being combined and processed across the business of the merged entity.

Though this discussion is necessarily general and example-based, the specific context of each remedy will be deeply important to understanding how data and privacy may be affected. As the 2019 Crémer Report to the European Commission on competition policy in the digital era explains, "any discussion of access to data must take into account the heterogeneity of data (along many dimensions), of use cases, of desired access conditions, etc. Discussing access to data in the abstract is futile."[516]

This need for case-specific understanding, and the growing relevance of data privacy to certain antitrust remedies, creates an opportunity for productive collaboration between antitrust and data privacy authorities. Though this intersection remains relatively new and rare, the expertise of data privacy authorities could provide valuable insight for antitrust authorities seeking to understand whether and when data privacy rights or interests are likely to be impacted by an antitrust remedy in a particular case. Such expertise could highlight privacy impacts, and inform the design or implementation of antitrust remedies in a manner that limits or reduces unnecessary effects of antitrust remedies on data privacy. In fact, the OECD has specifically called for

[514] Canadian Competition Bureau, *Statement Regarding McKesson's Acquisition of Katz Group's Healthcare Business* (Dec. 16, 2016)**,** https://www.competitionbureau.gc.ca/eic/site/cb-bc.nsf/eng/04174.html (finding the combination of datasets by the merging parties was likely to result in coordinated effects on competition, and requiring a data firewall that restricts the transmission of data between the various parts of the merged entity's business); Dept. of Justice, *Justice Department Requires Ticketmaster Entertainment Inc. to Make Significant Changes to Its Merger with Live Nation Inc.* (Jan. 25, 2010), https://www.justice.gov/opa/pr/justice-department-requires-ticketmaster-entertainment-inc-make-significant-changes-its (requiring firewalls between the data of the merging parties to prevent the merged firm from using information obtained from its ticketing business in operations of its promotions or artist management business, and also requiring that the merger firm permit clients to port their data to another ticketing service).

[515] Eur. Comm'n Press Release IP/20/2484, Mergers: Commission Clears Acquisition of Fitbit by Google, Subject to Conditions (Dec. 17, 2020).

[516] Crémer Report, *supra* note 110 at 73.

cooperation in the design of remedies: "[w]here behavioural remedies in competition law are pursued, perhaps to clarify unclear aspects of privacy and data protection and consumer law, such remedies should be drafted in cooperation and consultation with the privacy and data protection and consumer authorities."[517]

Further, the remedies employed in the context of data privacy enforcement could provide insights for the design of innovative data-related remedies in antitrust law. The Dutch data protection authority, for example, implemented a "compare and forget" method of data matching in its enforcement against WhatsApp, a popular messaging app.[518] The remedy permitted WhatsApp to have short term, read-only access to user contact lists, which enabled users to identify which of their existing contacts also used WhatsApp. After this contact matching occurred, the contact information was deleted. Such solutions might help new entrants to compete with incumbents, while also minimizing the potentially unnecessary privacy effects of long term data collection and use. Inter-agency collaboration is imperative to achieve innovative antitrust remedies that account for data privacy rights and interests and advance the interests of both realms.

Future Topics for Discussion and Collaboration Across the Antitrust and Privacy Spheres

As this Report reflects, this interaction of law is complex, new and often under-theorized. There are many topics where the antitrust/data privacy intersection would benefit from further development of theory and practice. Throughout the discussion, the Report suggests various subject areas where collaboration between antitrust and data privacy authorities would be particularly valuable. The following list consolidates those suggestions, and adds more pointed discussion questions. These high-priority topics for future cross-agency discussion include:

1. Privacy Quality and Competition: **Are there tradeoffs between the promotion of competition and the protection of data privacy in law, enforcement or policy? If so, when and to what extent are such tradeoffs likely to occur? How might agencies in each realm assess and understand those tradeoffs?**

   As discussed in this Report, it is important to identify and understand whether and when there are truly policy choices or tradeoffs between the promotion of competition and the

[517] OECD, Zero-Price Economy – Annex, *supra* note 22, at 5.

[518] EDPS Preliminary Op., Big Data 2014, *supra* note 346 (discussing Dutch DPA remedy against WhatsApp in 2013 case).

protection of data privacy, and when both might be optimized. It would be particularly useful to identify important privacy/competition tradeoffs in the digital economy. To the extent tradeoffs exist between the interests of data-driven competition and data protection, cross-agency discussion would be useful to understand how each realm views the appropriate balance between the two interests. Though views on the correct balance may justifiably differ, the purpose of the discussion is not to create consensus. Instead, it is intended to promote deliberate and careful thinking, and to build a shared understanding across each realm that could reduce unwitting or unnecessary tradeoffs as each enforcer pursues their respective mandate.

2. Privacy Quality and Competition: **When is the quality of privacy protection within a market likely to be affected by competition? How is such privacy quality likely to be affected? Conversely, when might data privacy protection affect competition?**

   It would be helpful for antitrust and data privacy authorities to discuss and develop understandings of whether (and when) privacy-based competition might be expected to impact the privacy features and quality of products in particular markets, and when it may not. Further, it would be helpful to develop evidence to substantiate the understanding of this relationship between privacy quality and competition. Shared policy issues across both realms may well impact the responses to these questions, such as the role of consumer bias, information asymmetry and the often limited and complex privacy choices faced by consumers.

3. Measuring Competitive Effects on Privacy**: In practical terms, how might antitrust authorities measure the relevant effects of competition on the quality of privacy offered in a given market?**

   There have been few recent developments in antitrust quantification of quality-based effects. In particular, the methods and tools for measuring the effects of competition on privacy are at a nascent stage, yet play a central role in the integration of privacy consideration into many aspects of antitrust analysis. There is a significant opportunity for collaboration between data privacy and antitrust authorities to develop reliable, well-founded methodology and tools to measure competition-related effects on privacy quality. In particular, the expertise of data privacy authorities in the measurement and evaluation of privacy, and the effects of market conduct on privacy levels could provide important insight to antitrust authorities seeking to evaluate privacy-based effects on competition.

4. Abuse of Dominance: **What is the relationship between monopolization, competition and privacy? How might monopoly power, or conversely, competition, affect the privacy protections offered to consumers? What evidence exists to substantiate and understand the views on this relationship?**

   Cases are beginning to allege that the exercise of monopoly power reduces the quality of privacy offered by services in certain markets. This raises an important opportunity to develop a well-substantiated and deeper understanding of the relationship between monopolization and privacy. This topic relates to the prior discussion topic, and would similarly benefit from evidence-based approaches.

5. Business Justifications: **When, if ever, does the protection of data privacy justify otherwise anticompetitive conduct? How might antitrust authorities properly evaluate arguments that a merger or misconduct was engaged in to protect the data privacy of individuals?**

   Data privacy is beginning to be claimed as a business justification for anticompetitive conduct. Collaboration between antitrust and data privacy authorities would be productive in assessing such claims. Privacy expertise could inform the antitrust determination of whether there are in fact legitimate privacy interests at stake, and ensure an accurate understanding of the scope of those privacy interests in specific cases. Privacy expertise would also be helpful in determining whether companies are over-interpreting data privacy compliance obligations in order to limit competition.

6. Mergers: **How is privacy quality, as it relates to competition, likely to be impacted by mergers or other transactions? What are the accepted theories regarding the effects of mergers, and other corporate transactions, on privacy-related competition?**

   There have now been several merger reviews that have considered the impacts of competition on privacy, making this one of the more developed touchpoints between the two areas of law. However, the role of data privacy in merger reviews remains at a stage of early investigation, theory and understanding. As the regulators with the deepest expertise on privacy, privacy agencies could contribute valuable insight on the likely effects of mergers on privacy-based competition in specific cases, and the development of sound theories of merger-related effects.

7. Remedies: **How is data privacy relevant to various types of antitrust remedies? How might antitrust remedies be designed to limit unnecessary or unintentional effects on data privacy, particularly where remedies mandate the disclosure of personal**

data, or impose interoperability obligations on companies that hold personal data?

As antitrust authorities consider and impose data-related remedies that involve personal information, privacy will increasingly become a consideration in the design of those remedies. Though this intersection remains relatively new and rare, the expertise of data privacy authorities could provide significant insight for antitrust authorities seeking to understand whether and when data privacy rights or interests are likely to be impacted by antitrust remedies in particular cases. Such expertise could also inform the design or implementation of remedies in a manner that limits unnecessary effects of such remedies on data privacy.

8. Assessment and Development of Theories and Practice: **As existing theories on antitrust and data privacy are tested and developed in enforcement and litigation, are those theories proving well-founded, evidence-based and sufficiently broad to explain the various interactions between the two areas of law? Recognizing that this is a nascent intersection of law, how might developments in data privacy or antitrust law (or policy) affect the interactions between these two realms?**

   This is a rapidly developing intersection of law. The thinking here is new, and would benefit from ongoing evaluation, as it is tested, developed and expanded in cases and enforcement.

   Around the world, some jurisdictions are passing their first data privacy laws. Existing laws are being expanded through new amendments and enforcement action. At the same time, antitrust law is also being amended with an eye to greater digital enforcement, and antitrust agencies around the world are bringing novel cases against digital platforms. This expansion of both areas of law may create new or more extensive interactions between them, as well as with consumer protection law. As several jurisdictions consider and introduce *ex ante* digital sector regulation, both antitrust and data privacy agencies may also find themselves collaborating with a new agency or new law that affects this shared space. Effective cross-agency collaboration will require antitrust and data privacy enforcers to keep pace with these developments.

Conclusion

This Report illustrates the wealth of new and varied interactions between antitrust, competition and data privacy. A simple assumption of complementarity or tension between the two legal regimes belies their multi-faceted nature, and likely does a disservice to both. Instead, the story is

one of many nuanced touchpoints between antitrust, privacy and competition, with more still emerging. The Report works to describe this landscape based on the perspectives of data privacy and antitrust enforcement authorities, both in terms of the challenges and the opportunities.

Though the fact of interaction between data privacy and competition is increasingly understood, the practice and details of its operation in policy and enforcement remain largely unsettled. The analytical theories here are at an early stage, with much room for development. As agencies rise to meet the global challenge of digital regulation, this interaction will only expand in frequency, complexity and scope. The next frontier will require the sharing of expertise across both agency realms, to build concrete, evidence-based theories and a deep, effective understanding of this legal intersection, in theory and in practice.

As this Report attests, data protection and competition authorities cannot achieve their goals in isolation. To advance theory and practice at this intersection, there is a growing need, and many significant opportunities, for multi-disciplinary collaboration among antitrust and data privacy enforcers. Cross-doctrinal cooperation will be essential to achieve cohesive and effective digital regulation, and all of its concomitant benefits for the economy, consumers and even the agencies themselves. Now is the time for careful consideration, and collaboration, to shape the new antitrust/data privacy interface.

Annex 3.

DCCWG Mapping of Regulatory Intersections and Actual Collaborative Actions Table

Mapping of intersections and collaborative actions across regulatory spheres

1. Actual collaborative action

This table captures concrete examples of joint regulatory initiatives or actions undertaken by competition and anti-trust authorities, and/or consumer protection authorities, and privacy and data protection authorities to consider or address intersection issues that span the regulatory spheres.

Date	Jurisdiction/s or organisation/s	Area of intersection	Description	Outcome	Status (DCCWG previously reported on this)
June 2021	**United Kingdom** The Competition and Markets Authority	Competition/ anti-trust and privacy	**The UK Competition and Markets Authority (CMA) is investigating Facebook's use of ad data** • The CMA has launched a probe into whether Facebook has gained an unfair advantage over competitors in providing services for online classified ads and online dating, through how it gathers and uses certain data. • The CMA will look into whether Facebook has unfairly used the data gained from its advertising and single sign-on to benefit its own services, in particular Facebook Marketplace - where users and businesses can put up classified ads to sell items - and Facebook Dating - a dating profile service it launched in Europe in 2020. GOK UK.	Investigation	New
June 2021	**United Kingdom and European Union** The U.K's Competition and Markets Authority and the European Commission	Competition/ anti-trust and privacy	**European Commission is investigating possible anti-competitive conduct of Facebook** • The European Commission has opened a formal antitrust investigation to assess whether Facebook violated EU competition rules by using advertising data gathered in particular from advertisers in order to compete with them in markets where Facebook is active such as classified ads. • The formal investigation will also assess whether Facebook ties its online classified ads service "Facebook Marketplace" to its social network, in breach of EU competition rules. European Commission.	Investigation	New
May 2021	**International Consumer Protection and Enforcement Network (ICPEN)**	Consumer protection and privacy	**ICPEN members successfully ensure that Apple and Google provide consumers with clear information on data collection and sharing practices** • In 2018 and 2019, ICPEN members (lead by Consumer Authority of Norway, the UK Competition and Markets Authority and the Netherlands Authority for Consumers and Markets) sent a joint letter to Apple and Google pressuring them to make changes to their app stores, in order to improve the information available on the use	Joint Action	New

Date	Jurisdiction/s or organisation/s	Area of intersection	Description	Outcome	Status (DCCWG previously reported on this)
			of personal data by apps available on their app stores (Apple App store and Google Play store). • As a result of the joint action, ICPEN members have managed to ensure that Apple and Google must provide consumers with clear and comprehensive information enabling consumers to compare and choose apps based on how they use personal data. Google will make this mandatory for all apps from 2022 onward. Apple already made similar changes in 2020. ICPEN News release. Forbrukertilsynet.		
May 2021	**Brazil** The Administrative Council for Economic Defense (Cade), the Federal Public Ministry (MPF), the National Data Protection Authority (ANPD) and the National Consumer Secretariat (Senacon)	Competition/ anti-trust, consumer protection and privacy	**Brazilian regulators have issued a joint recommendation to WhatsApp to postpone implementing its new privacy policy** • Brazil's data protection agency, competition authority, national consumer protection authority, and Federal Prosecution Service issued a joint recommendation to WhatsApp and Facebook seeking that they postpone the introduction of its privacy policy, amid privacy and consumer rights concerns. The concerns raised include: o the effects on competition, stemming from the WhatsApp policies, noting a lack of meaningful alternatives to Facebook's services o the effects on consumer protection, where there is an absence of clear information about what data will be processed and the purpose of the processing operations that will be carried out. • The recommendations outlined by the Brazilian authorities include: o delaying the roll-out of the privacy policy (due to be implemented on 15 May), until several points that have emerged during the bodies' scrutiny of the new privacy framework are addressed o that WhatsApp continue to provide services without restrictions to users that refuse to accept the new policy. GOV BR. ZDNet.	Joint Recommendation	New
May 2021	**United Kingdom** The Information Commissioner's Office (ICO) and the Competition and Markets Authority (CMA)	Competition/ anti-trust, and privacy	**ICO and CMA set out blueprint for cooperation in digital markets** • The UK ICO and CMA have published a joint statement setting out their shared views on the relationship between competition and data protection in the digital economy. • The statement affirms the ICO and CMA's commitment to working together to maximise regulatory coherence and promote outcomes which simultaneously promote competition and enhance data protection and privacy rights. They will do this through:	Joint Statement	New

Date	Jurisdiction/s or organisation/s	Area of intersection	Description	Outcome	Status (DCCWG previously reported on this)
			o work of the Digital Regulatory Cooperation Forum (DRCF) – see below for further details o continuing engagement with respective international counterparts o ongoing collaboration between ICO and CMA, particularly on their shared projects such as the CMA's investigation into Google's Privacy Sandbox proposals and the ICO's into real time bidding and the AdTech industry.		
April 2021	**Australia** Australian Competition and Consumer Commission (ACCC)	Competition/ anti-trust, consumer protection and Privacy	**ACCC inquiry into Digital Platforms** • In February 2020 the Australian Government directed the ACCC to conduct an inquiry into markets for the supply of digital advertising technology services and digital advertising agency services. • In April 2021, the ACCC published its second interim report, which found that Apple's App Store and Google's Play Store have significant market power in the distribution of mobile apps in Australia, and measures are needed to address this. • While the scope of the Inquiry has focussed mainly on markets for the supply of digital platform services in Australia and their impacts on competition and consumers, the ACCC's first and second interim reports have considered issues such as the reported tension between consumer privacy and transparency and competition, and the impact of data practices (including their ability to collect information about consumers) of app marketplaces on competition. The ACCC's third report is due in September 2021 and the final report is due in August 2021. ACCC press release.	Second Inquiry Report	New
April 2021	**United Kingdom** Competition and Markets Authority (CMA)	Competition/ anti-trust, consumer protection and privacy	**UK commences Digital Markets Unit** • In November 2020, the UK Government announced that a new competition regime will be set up which includes the introduction of the Digital Markets Unit (DMU) within the Competition Markets Authority (CMA) and a statutory code of conduct. • The DMU will oversee plans to give consumers more choice and control over their data over personal data held by market-leading platforms, promote online competition and crack down on unfair practices which can often leave businesses and consumers with less choice and more expensive goods and services. • The DMU has commenced activity in April 2021 and will work closely with the ICO, Ofcom and the Financial Conduct Authority so that consumers and businesses are comprehensively protected and the new regime is coherent and effective. GOK UK press release.	Competition Regime	New

Date	Jurisdiction/s or organisation/s	Area of intersection	Description	Outcome	Status (DCCWG previously reported on this)
April 2021	**Italy** **Council of State**	Competition/ anti-trust, and privacy	**Italy fines Facebook million for competition and data issues** • Italy's Council of State, which has jurisdiction on acts of all administrative authorities, has fined Facebook €7 million for not complying with a request to correct improper commercial practices in its treatment of user data. The decision of 29 March says that given the economic value of the data for Facebook, Facebook users should have been able to decide for themselves whether their data should be used. Facebook had misled users to register on the Facebook platform without informing them that their data would be used for commercial purposes.	Judgment	New
March 2021	**Germany** Bundeskartellamt (competition regulator)	Competition/ anti-trust, and privacy	**Germany's Bundeskartellamt prohibits Facebook from combining user data from different sources** • The European Court of Justice has been asked to clarify whether Germany's competition authority was right to order Facebook to halt its data collection practices, due to concerns over alleged abuse of its dominant market position and violations of EU data protection law. • In 2019, Germany's Federal Cartel Office (Bundeskartellamt) imposed restrictions on Facebook's sharing of data between its own platforms Facebook, Instagram and WhatsApp as well as third-party apps, claiming that the extent to which Facebook collects data without the consent of the user and shares it between its services is an abuse of power. The Bundeskartellamt's decision caused Facebook to appeal the decision to the Düsseldorf Higher Regional Court. In response, the authority lodged its own appeal with the federal Supreme Court in Karlsrühe, which ruled provisionally in favour of the Bundeskartellamt's restriction order. • Following this, the case went back to the Düsseldorf court, where it made inconclusive findings: *"The question of whether Facebook is abusing its dominant position as a provider on the German market for social networks because it collects and uses the data of its users in violation of the GDPR cannot be decided without referring to the [Court of Justice of the European Union]."* The court will make a formal submission to the Court of Justice of the European Union on this matter. Decision	Bundeskartellamt's decision	New
February 2021	**European Union**	Consumer protection and privacy	**TikTok and the European Consumer Organisation (BEUC)** • The European Consumer Organisation (BEUC) has lodged with the European Commission and the bloc's network of consumer protection authorities a complaint	Complaint lodged	New

Date	Jurisdiction/s or organisation/s	Area of intersection	Description	Outcome	Status (DCCWG previously reported on this)
			against the video-sharing site, while consumer organisations in 15 countries have alerted their national authorities and urged them to investigate the social media giant's conduct, BEUC stated. • Based on the findings of new research, BEUC contends that TikTok falls foul of multiple breaches of EU consumer rights and fails to protect children from hidden advertising and inappropriate content: o Several terms in TikTok's 'Terms of Service' are unfair o TikTok's 'Virtual Item Policy' which manages this feature contains unfair terms and misleading practices. o TikTok fails to protect children and teenagers from hidden advertising and potentially harmful content on its platform o TikTok's practices for the processing of users' personal data are misleading.		
November 2020	**Germany** Bundeskartellamt (competition regulator)	Consumer protection and privacy	**The Bundeskartellamt will launch a sector inquiry into messenger services** • The Bundeskartellamt has launched a sector inquiry into messenger services under consumer protection law. • Messenger services enable consumers to send text messages, photos and videos or make telephone calls via the internet. Surveys and media reports have repeatedly pointed out possible violations of consumer protection law in this sector: In some cases the way in which established messenger services manage the personal data of their users could be in violation of applicable data protection rules. Consumers must also be correctly informed about the measures taken to ensure secure communication. As to the interoperability of messenger services that has been repeatedly called for, the Bundeskartellamt hopes to be able to gain insights as to whether improvements in this area can result in an increased use of more privacy-friendly services. Bundeskartellamt press release.	Inquiry	New
October 2020	**United States** Federal Trade Commission (FTC)	Competition/ anti-trust, consumer protection and privacy	**Report on enhancing cooperation between the FTC and overseas competition and consumer protection authorities** • The Federal Trade Commission (FTC) issued a report on a series of hearings, "Competition and Consumer Protection in the 21st Century". The session "The FTC's Role in a Changing World", co-sponsored by the George Washington University Law School Competition Law Center and organised by the FTC explored the FTC's international role in light of globalisation, technological change, and the increasing	Hearing and Report	New

Date	Jurisdiction/s or organisation/s	Area of intersection	Description	Outcome	Status (DCCWG previously reported on this)
			number of competition, consumer protection, and privacy laws and enforcement agencies around the world.		
July 2020	**United Kingdom** The Information Commissioner's Office (ICO), the Competition and Markets Authority (CMA), Ofcom (communications regulator) and the Financial Conduct Authority	Competition/ anti-trust, privacy and communications	**The UK established a Digital Regulation Cooperation Forum which comprises CMA, ICO, Ofcom and the FCA** • The UK has established a new forum – the Digital Regulation Cooperation Forum - to help ensure online services work well for consumers and businesses in the UK. The Forum comprises the privacy, competition, communications and financial regulators – the FCA officially joined on 1 April 2021. • The Digital Regulation Cooperation Forum strengthens existing collaboration and coordination between the four regulators. It aims to harness their collective expertise when data, privacy, competition, communications and content moderation interact. Bringing together their collective knowledge, the Forum will help to coordinate action and support the development of informed, cohesive and responsive regulation. • The Forum has been created in recognition of the "unique challenges posed by digital markets and services" and the recognition that "regulatory cooperation has never been so important." The regulators have published a workplan which set out the DRCF's priorities for the next financial year (2021-2022).	Forum to promote regulatory cooperation	Existing[10]
July 2020	**Philippines** National Privacy Commission	Consumer protection and privacy	**NPC issue Public Health Emergency Bulletin as Guidance for Establishments** • The NPC issued a Public Health Emergency Bulletin as Guidance for Establishments on the Proper Handling of Customer and Visitor Information for Contact Tracing • Pursuant to the Memorandum Circulars of the Department of Trade and Industry (Circular 20-28 s. 2020 and Circular 20-37, s. 2020) on the Guidelines to Follow on Minimum Health Protocols for Establishments, the NPC issued a bulletin to guide establishments on the proper handling and protection of personal data collected from customers and visitors.	Guidance	Existing[11]

[10] This activity was captured in the DCCWG's 2020 Final Report p. 12.

[11] This activity was captured in the DCCWG's 2020 Final Report p. 8.

Date	Jurisdiction/s or organisation/s	Area of intersection	Description	Outcome	Status (DCCWG previously reported on this)
			• The bulletin reminds businesses to ensure that processing of personal data is proportional to the purpose of contact tracing, and collect only information required under existing government issuances. • The guidance reiterated that establishments should inform their customers and visitors on the reason for the collection and use personal data only for such declared purpose. • All establishments that collect personal information, whether through physical or electronic means have the obligation to implement reasonable and appropriate safeguards to protect customer data against any accidental or unlawful processing, alteration, disclosure and destruction.		
2020/21, 2018/19, 2017/18	**Canada** Office of the Privacy Commissioner (OPC) and the Competition Bureau (CB)	Competition/ anti-trust, consumer protection and privacy	**OPC facilitated staff secondments from the Competition Bureau** • The OPC has accepted secondees from the Competition Bureau (CB) to enhance cross-regulatory knowledge across all three of the regulatory spheres of privacy and data protection, competition, and consumer protection, and to benefit from the Bureau staffs' professional skills and investigative approach. • Three Competition Bureau Officers have participated in this formal staffing arrangement since 2017.	Secondment	Existing[12]
June 2020	**Australia** Office of the Australian Information Commissioner (OAIC) and Australian Competition and Consumer Commission (ACCC) and the e-Safety Commissioner	Competition/ anti-trust, consumer protection, and privacy	**Joint Directory of Online Safety and Security Services** • The OAIC is contributing to a Joint Directory of Online Safety and Security Services with the ACCC, the e-Safety Commissioner and the Australian Cyber Security Centre.	Directory	Existing[13]

[12] This activity was captured in the DCCWG's 2020 Final Report p. 3.

[13] This activity was captured in the DCCWG's 2020 Final Report p. 3.

Date	Jurisdiction/s or organisation/s	Area of intersection	Description	Outcome	Status (DCCWG previously reported on this)
	and the Australian Cyber Security Centre				
May 2020	**Australia** Office of the Australian Information Commissioner (OAIC) and Australian Competition and Consumer Commission (ACCC)	Competition/ anti-trust and privacy	**ACCC and OAIC Consumer Data Right Compliance and Enforcement Policy released** • The ACCC and OAIC jointly released the Compliance and Enforcement Policy for Australia's Consumer Data Right scheme. The Policy outlines the approach that the ACCC and the OAIC have adopted to encourage compliance with, and address breaches of, the Consumer Data Right regulatory framework. The Policy has been developed following consultation with current and future data holders and recipients. OAIC press release.	Joint Policy	Existing[14]
April-December 2020	**United Kingdom** The Information Commissioner's Office (ICO) and the Competition and Markets Authority (CMA)	Competition/ anti-trust and privacy	**ICO facilitated staff secondment to the UK Competition and Markets Authority** • The ICO seconded staff to the UK CMA's Digital Markets Taskforce to consider and provide input on the privacy aspects of advice to the UK government on pro-competitive initiatives for digital markets and platforms. • The Digital Markets Taskforce published its advice to government on the potential design and implementation of pro competitive measures for unlocking competition in digital markets on 9 December 2020.	Secondment	Existing[15]
March 2020	**United States** Federal Trade Commission (FTC)	Competition/ anti-trust and privacy	**FTC and U.S. Department of Justice Joint Statement** • The FTC and the U.S. Department of Justice Antitrust Division issued joint statement detailing an expedited antitrust procedure and providing guidance for collaborations of businesses working to protect the health and safety of Americans during the COVID-19 pandemic. FTC press release.	Joint statement	Existing[16]

[14] This activity was captured in the DCCWG's 2020 Final Report p. 4.

[15] This activity was captured in the DCCWG's 2020 Final Report p. 4.

[16] This activity was captured in the DCCWG's 2020 Final Report p. 4.

Date	Jurisdiction/s or organisation/s	Area of intersection	Description	Outcome	Status (DCCWG previously reported on this)
February 2020	**Norway** The Norwegian Data Protection Authority (Datatilsynet) and the Norwegian Consumer Authority	Consumer protection and privacy	**Datatilsynet and Norwegian Consumer Authority's Joint Guidance on Digital services and consumer personal data** • In 2018, the Norwegian Data Protection Authority (Datatilsynet) and the Norwegian Consumer Protection Authority (Forbrukertilsynet) drew up a common framework that they use as a starting point in evaluating how different issues related to consumer data and data-based business models can be resolved pursuant to data protection and consumer rights legislation. • The Datatilsynet and the Norwegian Consumer Authority developed and published jointly a guide on digital services and consumer personal data (the Guide). The Guide aims to help business operators, developers, marketers and providers of digital services navigate practical issues where consumer protection and privacy issues overlap. • Several areas the Guide addresses includes the marketing of digital services, the legal basis for the processing of personal data, the use of data for targeted marketing purposes, and the protection of children and young consumers. Datatilsynet's press release and the Consumer Authority's press release.	Joint guidance	Existing[17]
November 2019	**Australia** Office of the Australian Information Commissioner (OAIC) and Australian Competition and Consumer Commission (ACCC)	Consumer protection and privacy	**ACCC and OAIC joint workshop on cloud computing technology** • The ACCC and the OAIC organised a joint workshop to explore and understand further cloud computing technology. The workshop was facilitated by Amazon Web Services.	Joint workshop	Existing[18]
December 2017-July 2019	**Australia** Australian Competition and	Competition/ anti-trust, consumer	**ACCC inquiry into Digital Platforms**	Inquiry and Final Report	Existing[19]

[17] This activity was captured in the DCCWG's 2020 Final Report p. 4.

[18] This activity was captured in the DCCWG's 2020 Final Report p. 5.

[19] This activity was captured in the DCCWG's 2020 Final Report p. 5.

Date	Jurisdiction/s or organisation/s	Area of intersection	Description	Outcome	Status (DCCWG previously reported on this)
	Consumer Commission (ACCC)	protection and Privacy	• In December 2017, the Australian Government tasked the ACCC with undertaking an Inquiry into the practices of Digital Platforms. • While the scope of the Inquiry focussed mostly on the impact of Digital Platforms on the media industry, there was significant consideration given to the information handling practices of Digital Platforms. • The OAIC collaborated closely with the ACCC on this aspect of the ACCC's Inquiry and final report to Government. The OAIC also provided a public submission to the ACCC's preliminary report. ACCC press release.		
August 2019	**Norway** The Norwegian Data Protection Authority (Datatilsynet), the Norwegian Consumer Protection Authority (Forbrukertilsynet) and the Norwegian Competition Authority (Konkurransetilsynet)	Competition/ anti-trust, consumer protection, and privacy	**Cooperation forum between Norwegian Data Protection authority, Consumer Protection authority and Consumer Council** • In August 2019, a first meeting was held between Datatilsynet, Forbrukertilsynet and the Norwegian Competition authority (Konkurransetilsynet) in a new cooperation forum. All three authorities have seen the importance of working together to strengthen consumer rights in the digital economy. • In October 2020, the three authorities held a public webinar regarding big tech platforms and the digital market together with the Norwegian Consumer Council (Forbrukerrådet) • In April 2021, the cooperation forum was formalized as the "Forum on the digital economy". The forum has four meetings each year.	Regulatory co-operation	Existing[20]

[20] This activity was captured in the DCCWG's 2020 Final Report, p.6.

2. Regulatory intersection:
Enforcement and regulatory activity

This table captures instances where competition or anti-trust authorities, consumer protection authorities, or privacy and data protection authorities have undertaken enforcement and regulatory activity to address an intersection matter or issue, outside their traditional regulatory sphere. The range of activities undertaken includes, but is not limited to, investigations, assessments/audits, civil penalty orders, enforceable undertakings, monetary penalties, remedial directions, legal proceedings or complaints raised.

Date	Jurisdiction/s or organisation/s	Area of intersection	Description	Outcome	Status (DCCWG previously reported on this)
May 2021	**Germany** Bundeskartellamt (competition regulator)	Competition/ anti-trust and privacy	**Germany's competition regulator (the Bundeskartellamt) has initiated two proceedings against Google, based on new competition law provisions applicable to digital companies** • In January 2021, the 10th amendment to the German Competition Act (GWB Digitalisation Act) came into force. A key new provision (Section 19a GWB) enables the Bundeskartellamt to intervene earlier and more effectively, in particular against the practices of large digital companies. Under the amendment, the Bundeskartellamt can prohibit companies which are of paramount significance for competition across markets from engaging in anti-competitive practices. • One of the proceedings will determine whether the amended competition rules apply in its case (ie. To determine if Google is a company of 'paramount significance'), and which would enable the Federal Cartel Office (FCO) to target it with proactive interventions in the interests of fostering digital competition. • The second, is a parallel procedure involving the Federal Cartel Office (FCO) undertaking an in-depth analysis of Google's data processing terms, on a working assumption that Google/Alphabet's business meets the legal bar in the GWB Digitalisation Act. Bundeskartellamt. Yahoo Finance.	Legal Proceedings	New

Date	Jurisdiction/s or organisation/s	Area of intersection	Description	Outcome	Status (DCCWG previously reported on this)
May 2021	**Argentina** National Commission for the Defence of Competition (CNDC) of Argentina and the Secretariat of Internal Trade of the Ministry of Production	Competition/ anti-trust and privacy	**National Commission for the Defence of Competition (CNDC) orders Whatsapp to suspend the implementation of WhatsApp's new Terms of Service and Privacy Policy** • The CNDC issued a report raising concerns over Whatsapp's new terms of service and privacy policy, which was due to be implemented on 15 May 2021. • As a result of the changes, users who do not accept the policy will experience limitations and eventually lose functionality of the service, which generates a strong asymmetry in the negotiating power between users and WhatsApp as, users are mostly 'forced' to accept the new terms that enable WhatsApp to collect excessive personal information and share it with other entities such as Facebook and Instagram. • The CNDC found that the power of the information will allow Facebook and Instagram to reinforce their dominant position in other markets such as online advertising, will raise entry barriers for other competitors and monopolise the market, and the new WA privacy policies could be in violation of Argentina's competition laws. • As a result of the report, the Secretariat of Internal Trade of the Ministry of Productive Development, issued a precautionary interim measure ordering Facebook to suspend the implementation of WhatsApp's new Terms of Service and Privacy Policy. While the precautionary measure is in place, the CNDC will be investigation the effect of the new terms of service and the sharing of any data to Facebook for commercial purposes. Argentina GOB.	Precautionary measure/order	New
April 2021	**Australia** Australian Competition and Consumer Commission (ACCC)	Consumer protection and privacy	**Federal Court finds that Google for mislead users about the collection of personal location data** • The Federal Court of Australia has found that Google LLC and Google Australia Pty Ltd (together, Google) misled some users about personal location data collected through Android devices for two years, from January 2017 to December 2018. • The ACCC had instituted the proceedings against Google in October 2019 alleging that the Google breached Australian Consumer Law, and engaged in misleading conduct and made false or misleading representations to consumers about the personal location data that Google collects, keeps and uses when certain Google Account settings were enabled or disabled. • The Court ruled in favour of the ACCC, finding that from January 2017 Google misrepresented to consumers setting up a new Google Account on their Android device, that its 'Location History' setting was the only setting that affected whether	Legal Proceedings	New

Date	Jurisdiction/s or organisation/s	Area of intersection	Description	Outcome	Status (DCCWG previously reported on this)
			Google collected, kept or used personally identifiable location data. However, another setting titled 'Web & App Activity', if left enabled, would allow Google to continue collecting personal location data, even if the consumer had disabled the 'Location History' setting. ACCC press release.		
March 2021	**India** The Competition Commission of India (CCI)	Competition/ anti-trust, consumer protection and privacy	**India's competition authority (CCI) orders an anti-trust investigation into Whatapp's privacy policy changes** • Under the order, the Director General must investigate (within 60 days) WhatsApp's new policy to "ascertain the full extent, scope and impact of data sharing through involuntary consent of users." • The basis of issuing the order was that WhatsApp's privacy policy and terms of service set out categories of information to be shared with Facebook that are too broad, vague and unintelligible, for example "information on how users interact with others (including businesses), and that such incomplete disclosures hid the actual data cost that uses incur for using WhatsApp services. • The CCI consider that WhatsApp breached anti-trust laws in the guise of policy update and given the nature of the privacy policy update (in that users must accept or lose functionality or use of the app), it merits detailed investigation 'in view of the market position and market power enjoyed by WhatsApp.' TechCrunch article. CCI order.	Investigation	New
January 2021	**Turkey** The Competition Board of Turkey (Rekabet Kurumu)	Competition/ anti-trust and privacy	**The Competition Board of Turkey has launched an investigation into WhatsApp and its data sharing practices with Facebook** • As a result of WhatsApp's new privacy policy which informs users that to be able to use the app, they must consent to the sharing of their data with Facebook companies, the Competition Board has launched an investigation into whether the updated privacy policy breaches Turkey's competition law. • Further, the Competition Board issued an interim measure ordering WhatsApp and Facebook to cease the changes to its privacy policy (due to be implemented from 8 February 2021), until its investigation is complete. Data Guidance.	Investigation and Interim Order	New
2021	**Colombia**	Consumer protection and privacy	**SIC Guide on Electronic Commerce** • The Superintendence of Industry and Commerce currently its currently working on the Consumer Protection Guide on Electronic Commerce 2021.	E-commerce Guideline in progress	New

Date	Jurisdiction/s or organisation/s	Area of intersection	Description	Outcome	Status (DCCWG previously reported on this)
	Superintendence of Industry and Commerce		• This guide will allow businesses to know their duties and rights as online suppliers while giving trust and confidence to online consumers in regard of their rights protection. • Also the guide is aimed to cover issues and matters related to the actors involved in e-commerce and the differences between them, together with their liability regimes, as well as the rights, duties and obligations that arise in this field of e-commerce and how to deal with or attend consumers' complaints, claims and demands under this framework. The work for this guide began in January 2021 and is expected to be ready by December of this same year. It is important to note that, although this is a joint action which is currently ongoing and for which its first draft version was published and available for comments on the website of the SIC from 29th of June 2021 to 8th of July 2021 (then extended until 15th of July 2021), the final version of the guide is not yet ready and available to all public and it cannot be shared with other authorities.		
August 2020	**Australia** Australian Competition and Consumer Commission (ACCC)	Consumer protection and privacy	**Federal Court orders HealthEngine to pay $2.9 million penalty for misleading and deceptive conduct** • In August 2019, the ACCC instituted proceedings in the Federal Court of Australia against online health booking platform HealthEngine for misleading and deceptive conduct relating to the sharing of consumer information with insurance brokers and the publishing of patient reviews and ratings. • HealthEngine admitted that between 30 April 2014 and 30 June 2018, it shared patient data of over 135,000 patients, including names, phone numbers, email addresses and date of birth, with private health insurance brokers without informed consent of the patients. • After admitting liability, the Court ordered HealthEngine pay $2.9 million in penalties and that the company contact affected consumers to inform how they can regain control of their personal information. • The financial penalty was issued in relation to the misleading conduct in sharing patient data and the publishing of misleading patient reviews on its website. ACCC press release.	Legal proceedings	New

Date	Jurisdiction/s or organisation/s	Area of intersection	Description	Outcome	Status (DCCWG previously reported on this)
July 2020	**Australia** Australian Competition and Consumer Commission (ACCC)	Competition/ anti-trust, consumer protection and privacy	**ACCC alleges Google misled consumers about the expanded use of personal data** • The ACCC has launched Federal Court proceedings against Google LLC, alleging Google misled Australian consumers to obtain their consent to expand the scope of personal information that Google could collect and combine about consumers' internet activity, for use by Google, including for targeted advertising. • The ACCC alleges Google misled consumers when it failed to properly inform consumers, and did not gain their explicit informed consent, about its move in 2016 to start combining personal information in consumers' Google accounts with information about those individuals' activities on non-Google sites that used Google technology, formerly DoubleClick technology, to display ads. • This meant this data about users' non-Google online activity became linked to their names and other identifying information held by Google. Previously, this information had been kept separately from users' Google accounts, meaning the data was not linked to an individual user. Google then used this newly combined information to improve the commercial performance of its advertising businesses. • The ACCC also alleges that Google misled consumers about a related change to its privacy policy. ACCC press release.	Legal proceedings	Existing[21]
June 2020	**Germany** German competition authority (Bundeskartellamt)	Competition/ anti-trust, consumer protection and privacy	**German court has ordered Facebook to stop merging data collected through its WhatsApp and Instagram subsidiaries or other websites, unless users explicitly agree** • The German Federal Court of Justice (BGH) ordered Facebook to stop merging data collected through its Whatsapp and Instagram subsidiaries or other websites unless users explicitly agree, in a legal victory for competition authorities. • Germany's Bundeskartellamt had told Facebook to rein in the data collecting in a landmark decision in 2019, but the social media giant appealed the order. In a fast-track proceeding, Germany's BGH agreed with the Bundeskartellamt in finding that Facebook was abusing its dominant position to force users to consent to all their data being collected. "Facebook does not allow for any choice," presiding judge Peter	Legal ruling	Existing[22]

[21] This activity was captured in the DCCWG's 2020 Final Report p. 7.

[22] This activity was captured in the DCCWG's 2020 Final Report p. 8.

Date	Jurisdiction/s or organisation/s	Area of intersection	Description	Outcome	Status (DCCWG previously reported on this)
			Meier-Beck said. Facebook must comply with the order while its appeal is pending in a lower court. • The Bundeskartellamt criticised Facebook in February 2019 for making the "unrestricted" data harvesting part of the website's terms of use. That meant people had to tick the box or opt out of being on Facebook altogether. The personal data picked up through Facebook's own platform, Whatsapp, Instagram and third-party websites serve to build up a user's profile for the purposes of targeted advertising, a key income source for the group. Financial Times.		
June 2020	**Australia** Australian Competition and Consumer Commission (ACCC)	Competition/ anti-trust and privacy	**ACCC's preliminary concerns with Google's proposed acquisition of Fitbit** • The ACCC has outlined its preliminary concerns with Google's proposed acquisition of Fitbit, stating that Google's access to consumer health data may raise entry barriers, further entrench its dominant position and adversely affect competition in several digital advertising and health markets. • The ACCC's Chair Rod Sims stated that "our concerns are that Google buying Fitbit will allow Google to build an even more comprehensive set of user data, further cementing its position and raising barriers to entry to potential rivals." ACCC press release and Reuters article.	Preliminary concerns	Existing[23]
May 2020	**Canada** Competition Bureau (CB)	Consumer protection and privacy	**Competition Bureau's Facebook settlement that saw Facebook pay a CAD$9.5 million penalty and costs over concerns about misleading privacy claims** • Facebook will pay a $9 million penalty after the Competition Bureau concluded that the company made false or misleading claims about the privacy of Canadians' personal information on Facebook and Messenger. Facebook will also pay an additional $500,000 for the costs of the Bureau's investigation." As part of the settlement, Facebook has agreed not to make false or misleading representations about the disclosure of personal information, including representations about the extent to which users can control access to their personal information on Facebook and Messenger. Competition Bureau press release.	Investigation Monetary penalty Behavioural Remedy	Existing[24]

[23] This activity was captured in the DCCWG's 2020 Final Report p. 8-9.

[24] This activity was captured in the DCCWG's 2020 Final Report p. 9.

Date	Jurisdiction/s or organisation/s	Area of intersection	Description	Outcome	Status (DCCWG previously reported on this)
May 2020	**United States** Arizona Attorney General	Consumer protection and privacy	**Arizona's proceedings against Google for deceptive and unfair practices to obtain users' location data** • The Arizona Attorney General filed a lawsuit in the Maricopa County Superior Court against Google LLC, under the Arizona Consumer Fraud Act, alleging that the company used deceptive and unfair practices to collect detailed information about its users, including physical locations, to target users for advertising. • According to the Attorney General, the collection of location data is often done without users' knowledge and consent. Reuters.	Legal proceedings	New
March 2020	**United States** Federal Trade Commission (FTC)	Consumer protection and privacy	**FTC's initiation of proceedings against Retina-X, stalking apps** • The FTC brought an action against a developer of stalking apps software, Retina-X, that allows purchasers to monitor the mobile devices on which they are installed, without users' knowledge. • In its complaint, the FTC alleged that Retina-X sold apps that required circumventing certain security protections implemented by the mobile device operating system or manufacturer, and do so without taking steps to ensure that the apps would be used only for legitimate and lawful purposes. FTC press release and ZDNet article.	Legal proceedings	Existing[25]
February 2020 (ongoing)	**European Union** European Commission (Competition)	Competition/ anti-trust and privacy	**EU anti-trust regulators consider Google and Fitbit acquisition** • EU antitrust regulators will decide by 20 July 2020 whether to clear Alphabet Inc-owned Google's US$2.1 billion bid for fitness trackers company Fitbit, a deal that has prompted concerns from consumer groups and privacy advocates. • While privacy concerns are not part of the EU antitrust review, the trove of health data generated from Fitbit devices used to monitor users' daily steps, calories burned and distance travelled and how Google plans to use it is expected to be a focus. European Commission press release and Reuters article.	Preliminary concerns	Existing[26]

[25] This activity was captured in the DCCWG's 2020 Final Report p. 9.

[26] This activity was captured in the DCCWG's 2020 Final Report p. 10.

Date	Jurisdiction/s or organisation/s	Area of intersection	Description	Outcome	Status (DCCWG previously reported on this)
January 2020	**United States** Federal Trade Commission (FTC), Consumer Financial Protection Bureau	Consumer protection and privacy	**FTC's Equifax data breach settlement** • In September of 2017, Equifax announced a data breach that exposed the personal information of 147 million people. • The company has agreed to a global settlement with the FTC, the Consumer Financial Protection Bureau, and 50 U.S. states and territories. • The settlement includes up to US$425 million to help people affected by the data breach. FTC press release.	Settlement established	Existing[27]
January 2020	**United States** Federal Trade Commission (FTC) and Department of Justice	Consumer protection and privacy	**FTC settlement of Mortgage Broker who posted personal information in response to negative reviews** • A California-based mortgage broker will pay $120,000 to settle FTC allegations that it violated the Fair Credit Reporting Act and other laws by revealing personal information about consumers in response to negative reviews posted on the review website Yelp. • In a complaint filed by the Department of Justice on behalf of the FTC, the FTC alleges that Mortgage Solutions FCS, Inc. (doing business as Mount Diablo Lending) and its sole owner, Ramon Walker, responded to consumers who posted negative reviews on Yelp by revealing their credit histories, debt-to-income ratios, taxes, health, sources of income, family relationships, and other personal information. Several responses also revealed reviewers' first and last names, according to the complaint. FTC press release.	Settlement established	Existing[28]
January 2020	**United States** Federal Trade Commission (FTC)	Consumer protection and privacy	**FTC charge Grand Teton Professionals** • The FTC charged Grand Teton Professionals with running a credit repair scheme that collected more than $6.2 million in illegal upfront fees and falsely claimed to repair consumers' credit. Among other things, the FTC alleged that the operation obtained	Injunctive relief	Existing[29]

[27] This activity was captured in the DCCWG's 2020 Final Report p. 10.

[28] This activity was captured in the DCCWG's 2020 Final Report p. 10.

[29] This activity was captured in the DCCWG's 2020 Final Report p. 11.

Date	Jurisdiction/s or organisation/s	Area of intersection	Description	Outcome	Status (DCCWG previously reported on this)
			sensitive consumer data, like Social Security numbers and dates of birth, for bogus credit repair services. FTC press release.		
January 2020	**France** Commission nationale de l'informatique et des libertés (CNIL)	Consumer protection and privacy	**CNIL impose fine of €50 million under the GDPR upon Google** • On 25 and 28 May 2018, the CNIL received group complaints from the None Of Your Business and La Quadrature du Net against Google for not having a valid legal basis to process the personal data of the users of its services, particularly for ads personalization activities. As a result of CNIL's inspections, the CNIL observed two breaches of the General Data Protection Regulation (GDPR) by Google. • The CNIL imposed upon Google a fine of €50 million under the GDPR for a lack of transparency, inadequate information and lack of valid consent regarding the personalization of ads. This fine was upheld by France's administrative court. CNIL press release and Reuters article.	Monetary penalty	Existing[30]
2019-2020	**United States** Federal Trade Commission (FTC)	Consumer protection and privacy	**FTC undertakes actions against entities that falsely claimed participation in Privacy Shield** • In eight separate actions, the FTC charged that 214 Technologies, Click Labs, DCR Workforce, Incentive Services, LotaData, Medable, SecurTest, and Thru falsely claimed participation in Privacy Shield. While the companies initiated Privacy Shield applications with the U.S. Department of Commerce, the companies did not complete the steps necessary to be certified as complying with the Framework. Because they failed to complete certification, they were not certified participants in the Framework, despite representations to the contrary. • In separate actions, the FTC charged that Empiristat, Global Data Vault, and TDARX falsely claimed participation in Privacy Shield. The companies had allowed their certifications to lapse while still claiming participation. Further, the companies failed to affirm that they would continue to apply Privacy Shield protections to personal information collected while participating in the program.	Legal proceedings	Existing[31]

[30] This activity was captured in the DCCWG's 2020 Final Report p. 11.

[31] This activity was captured in the DCCWG's 2020 Final Report p. 12.

Date	Jurisdiction/s or organisation/s	Area of intersection	Description	Outcome	Status (DCCWG previously reported on this)
			• As a part of the FTC's action against Cambridge Analytica, the FTC determined that the company falsely claimed to participate in Privacy Shield after allowing its certification to lapse.		
2019-2020	**Colombia** Superintendence of Industry and Commerce (SIC)	Consumer protection and privacy	**The SIC undertook a Monitoring and surveillance report regarding identity and data theft in ICT services:** • First a diagnosis was presented regarding possible identity theft for the acquisition of products and/or services related to telecommunications and postal services that gave rise to negative reports in the credit histories of users, as well as complaints about the handling of personal data. • The diagnosis was made in order to identify those operators of telecommunications (mobile or fixed telephony and internet and paid or community TV) or postal services (express courier, mail and money orders) with the highest number of complaints related to the type of impersonation, the cities where these complaints were concentrated, and the steps to be followed by the SIC so as to identify, address and act in view of these situations. • The results of the monitoring and surveillance exercise showed that the complaints with respect to personal data, for the typologies of impersonation and/or fraud, in the telecommunications sector, complaints increased by 64% in 2020 with respect to those filed in 2019. In response the telecommunications operators have been designing mechanisms that have been updated as different cases of fraud arise. By comparison, in the postal sector complaints are numerically low, although they have increased from one year to the next, going from 4 in 2019 to 11 in 2020.	Monitoring exercise	New
2019	**Colombia** Superintendence of Industry and Commerce (SIC)	Competition and privacy	**SIC Review of Joint Venture banks in Colombia** • The Competition Authority reviewed a proposal from three banks from Colombia: Bancolombia, Davivienda and Banco de Bogota, to provide digital identification processes and services to their clients as a joint venture. • This provided increased privacy to the bank's clients, security and control over their products, and also the facility to access the platforms and inclusion. This Joint Project was the first of its kind in Colombia.	Project Approved	New

Date	Jurisdiction/s or organisation/s	Area of intersection	Description	Outcome	Status (DCCWG previously reported on this)
December 2019	**United States** Federal Trade Commission (FTC)	Consumer protection and privacy	**FTC establishes a settlement with Unrollme regarding deceptive consumer practices** • The FTC settled allegations with Unrollme, an email management company, which deceived consumers about how it accesses and uses their personal emails. According to the FTC's complaint, Unrollme falsely told consumers that it would not "touch" their personal emails to persuade consumers to provide access to their email accounts. • The complaint allege that Unrollme shared consumers' email receives, which includes user's name, billing and shipping addresses and information about products or services purchased by the consumer, with its parent company, Slice Technologies. Slice Technologies used anonymous purchase information from Unrollme users' e-receipts for the market research analytics products it sells. FTC press release.	Settlement established	Existing[32]
December 2019	**United States** Federal Trade Commission (FTC)	Consumer protection and privacy	**FTC settlement established with Global Asset Financial Services Group** • The FTC shut down a phantom debt brokering and collection scheme in its case against Global Asset Financial Services Group. • The FTC charged the defendants with purchasing and collecting on counterfeit debts fabricated from misappropriated information about consumers' identities, and finances and debts purportedly owed on bogus "autofunded" payday loans. In numerous instances, defendants also disclosed consumers' purported debts to third parties. • The final orders imposed a combined judgment of more than $13 million, banned all the defendants from debt collection business and from misleading consumers about debt. They also prohibit the defendants from profiting from customers' personal information collected as part of the practices, and failing to dispose of such information properly. FTC press release.	Settlement established	Existing[33]

[32] This activity was captured in the DCCWG's 2020 Final Report p. 12.

[33] This activity was captured in the DCCWG's 2020 Final Report p. 13.

Date	Jurisdiction/s or organisation/s	Area of intersection	Description	Outcome	Status (DCCWG previously reported on this)
December 2019	**United States and United Kingdom** Federal Trade Commission (FTC) and Information Commissioner's Office (ICO)	Consumer protection and privacy	**FTC action against Cambridge Analytica for deceptive conduct** • The FTC filed an action against the data analytics company, Cambridge Analytica, its Chief Executive Officer, Alexander Nix, and app developer, Aleksandr Kogan for deceptive conduct. The FTC's complaint alleged that Cambridge Analytica, Nix and Kogan used false and deceptive tactics to harvest personal information from millions of Facebook users for voting profiling and targeting. The complaint alleged that app users were falsely told the app would not collect users' names or other identifiable information. • Kogan and Nix agreed to settlements with the FTC that restrict how they conduct any business in the future, and the Commission entered a default judgment against Cambridge Analytica. FTC press release. • The FTC collaborated with the United Kingdom's Information Commissioner's Office in its actions against Cambridge Analytica and Aleksandr Kogan and Alexander Nix, described above. To facilitate international cooperation in these cases, the FTC relied on key provisions of the U.S. SAFE WEB Act, which allows the FTC to share information with foreign counterparts to combat deceptive and unfair practices.[34]	Various settlements established Regulatory cooperation	Existing[35]
September 2019	**United States** Federal Trade Commission (FTC) and the New York Attorney General	Consumer protection and privacy	**Google and YouTube Will Pay Record $170 Million for Alleged Violations of Children's Privacy Law** • Google LLC and its subsidiary YouTube, LLC will pay a record $170 million to settle allegations by the FTC and the New York Attorney General that the YouTube video sharing service illegally collected personal information from children without their parents' consent. • The settlement requires Google and YouTube to pay $136 million to the FTC and $34 million to New York for allegedly violating the Children's Online Privacy Protection	Civil penalty settlement	Existing[36]

[34] https://www.ftc.gov/system/files/documents/reports/reports-response-senate-appropriations-committee-report-116-111-ftcs-use-its-authorities-resources/p065404reportprivacydatasecurity.pdf, pg. 18.

[35] This activity was captured in the DCCWG's 2020 Final Report p. 13.

[36] This activity was captured in the DCCWG's 2020 Final Report p. 15.

Date	Jurisdiction/s or organisation/s	Area of intersection	Description	Outcome	Status (DCCWG previously reported on this)
			Act (COPPA) Rule. The $136 million penalty is by far the largest amount the FTC has ever obtained in a COPPA case since Congress enacted the law in 1998. FTC press release.		
August 2019	**United States** Federal Trade Commission (FTC)	Consumer protection and privacy	**FTC settlement established with Career Education Corporation as a result of deceptive conduct** • The FTC obtained final orders against In the Career Education Corporation, a company that used deceptive lead generators to market their schools. The company's lead generators used deceptive tactics, such as posing as military recruiting websites, to induce consumers to provide their information online. Those websites promised consumers that the information submitted would not be shared with anyone else, but the lead generators sold that information to the defendants to market their schools. The final order imposes a $30 million judgment for consumer redress. FTC press release	Civil penalty settlement	Existing[37]
July 2019	**United States** Federal Trade Commission (FTC) and U.S. Department of Justice	Competition/ anti-trust and privacy	**FTC and U.S. Department of Justice settlement with Facebook for deceptive conduct** • The FTC and the U.S. Department of Justice finalised a settlement with Facebook. A previous complaint alleged that Facebook violated the FTC's 2012 order against the company by misrepresenting the control users had over their personal information and failing to institute and maintain a reasonable program to ensure consumers' privacy. It also alleged that Facebook deceptively failed to disclose that it would use phone numbers provided by users for two-factor authentication for targeted advertisements to those users. • The Facebook order imposed a $5 billion penalty, and a host of modifications to the Commission's order designed to change Facebook's overall approach to privacy. The $5 billion penalty against Facebook is the largest ever imposed on any company for violating consumers' privacy. FTC press release.	Civil penalty	Existing[38]

[37] This activity was captured in the DCCWG's 2020 Final Report p. 15.

[38] This activity was captured in the DCCWG's 2020 Final Report p. 16.

Date	Jurisdiction/s or organisation/s	Area of intersection	Description	Outcome	Status (DCCWG previously reported on this)
July 2019	**United States** Federal Trade Commission (FTC) and the New York Attorney General's Office	Consumer protection and privacy	**Final orders secured by FTC and New York Attorney General against Hylan Asset Management** • In Hylan Asset Management, the FTC and the New York Attorney General's Office charged two operations—Hylan Asset Management, LLC and its related companies and Worldwide Processing Group, and their principals with buying, placing for collection, and selling lists of phantom debts, including debts that were fabricated by the defendants or disputed by consumers. • The Commission alleged that the defendants obtained consumers' private financial information and then used it to convince consumers they were legitimate collectors calling about legitimate debts. • The FTC also alleged that, in numerous instances, the Worldwide defendants unlawfully communicated with third parties where they already possessed contact information for the consumer. • The FTC secured final orders banning the Hylan defendants from the debt collection industry and prohibiting the Worldwide defendants from unlawful debt collection practices. The orders prohibit all defendants from using customers' personal information and failing to properly dispose of that information. FTC press release.	Settlement established	Existing[39]
April 2019	**United States** Federal Trade Commission (FTC)	Consumer protection and privacy	**FTC initiated complaint against Unixiz, Inc.** • The FTC's complaint against Unixiz, Inc., doing business as i-Dressup.com alleged that the company and its principals violated COPPA by failing to obtain verifiable parental consent before collecting personal information from children under 13. • To gain access to all the features on the website, including the social networking features, users had to register as members by submitting a username, password, birthdate, and email address. If a user indicated he or she was under 13, the registration field asked for a parent's consent. If a parent declined to provide consent, the under-13 users were given a "Safe Mode" membership allowing them to login to access i-Dressup's games and features but not its social features.	Complaint	Existing[40]

[39] This activity was captured in the DCCWG's 2020 Final Report p. 17.

[40] This activity was captured in the DCCWG's 2020 Final Report p. 17.

Date	Jurisdiction/s or organisation/s	Area of intersection	Description	Outcome	Status (DCCWG previously reported on this)
			• The FTC alleges, however, that i-Dressup still collected personal information from these children, even if their parents did not provide consent. FTC press release.		
March 2019	**United States** Federal Trade Commission (FTC)	Consumer protection and privacy	**FTC examined the privacy practices of broadband providers** • The FTC issued orders to seven U.S. Internet broadband providers and related entities seeking information the agency will use to examine how broadband companies collect, retain, use, and disclose information about consumers and their devices. • The orders seek information about the companies' privacy policies, procedures, and practices. The orders were sent to AT&T's advertising subsidiary, Appnexus Inc.; Verizon Online LLC, Verizon's wireline advertising subsidiary; another Verizon advertising subsidiary, Oath Americas Inc, and Charter Communications Inc, the U.S.'s second largest cable provider. • The FTC is initiating this study to better understand Internet service providers' privacy practices in light of the evolution of telecommunications companies into vertically integrated platforms that also provide advertising-supported content. Under current law, the FTC has the ability to enforce against unfair and deceptive practices involving Internet service providers. FTC press release and update.	Study	Existing[41]
February 2019	**United States** Federal Trade Commission (FTC)	Consumer protection and privacy	**FTC settlement with Musical.ly of $5.7 million** • In 2019, Musical.ly, now known as TikTok, paid $5.7 million to settle charges that it violated COPPA by illegally collecting personal information from children. The complaint alleged the app was child-directed, and that many users self-identified as being under 13. FTC press release.	Settlement finalised	Existing[42]
2019	**Colombia –** Superintendence of Industry and Commerce (SIC)	Consumer protection and privacy	**The SIC published its guidelines regarding the processing of personal data for marketing purposes and for e-commerce.**	Guidelines	New

[41] This activity was captured in the DCCWG's 2020 Final Report p. 18.

[42] This activity was captured in the DCCWG's 2020 Final Report p. 19.

Date	Jurisdiction/s or organisation/s	Area of intersection	Description	Outcome	Status (DCCWG previously reported on this)
			• Colombian Data Protection Authority published in 2019 its guideline regarding the processing of personal data for marketing purposes. Considering that personal data is a fundamental input of advertising activities. • Data subjects are also consumer. Thus, their information must be adequately processed when companies are trying to sell their products and services in the market. E-commerce is the engine of the 21st century economy and personal data is the currency of the digital economy. The development of the activities covered by electronic commerce implies the collection, use or circulation of your personal data. Hence, the authority published some guidelines for an adequate processing of personal data in such matter.		
July 2018	**United States** Federal Trade Commission (FTC) and Nevada Attorney General	Consumer protection and privacy	**FTC and Nevada Attorney General's action against MyEx.com for soliciting "revenge porn" from individuals without their knowledge or consent** • A Nevada federal court permanently shut down the revenge porn site MyEx.com and ordered the operators to pay more than $2 million in an action brought by the FTC and the Nevada Attorney General (AG). The FTC and the Nevada AG charged the site and related individuals with violating federal and state laws by posting intimate pictures of people and their personal information without consent, as well as charging takedown fees to have the items removed. • MyEx.com was solely dedicated to revenge porn, the FTC and Nevada AG alleged, and published pictures, videos and information including names, addresses, employers and social media account information. The site also encouraged users to "Add Your Ex" and "Submit Pics and Stories of Your Ex." To have information or images removed, the defendants charged fees ranging from $499 to $2,800. Individuals who were featured on the site suffered real harm, the FTC and Nevada AG told the court, including lost jobs, threats and harassment, and the financial burden of having the information removed. • The federal court ordered that the site be permanently shut down, that the images and personal information be destroyed, and that the defendants pay more than $2 million in damages. The defendants are also banned from posting intimate images and personal information of others on a website without the subjects' notice and consent. FTC press release..	Legal proceedings	Existing[43]

[43] This activity was captured in the DCCWG's 2020 Final Report p. 19.

3. Regulatory intersection:
Policy initiatives

This table captures instances where competition or anti-trust authorities, consumer protection authorities, or privacy and data protection authorities have undertaken policy related activity to address an intersection matter or issue, outside their traditional regulatory sphere. The range of policy-related activities undertaken includes, but is not limited to, publications, statements, participation in public consultations, academic studies, projects, and capability building initiatives.

Date	Jurisdiction/s or organisation/s	Area of intersection	Description	Outcome	Status
July 2021	**Global Privacy Enforcement Network (GPEN)**	Consumer protection and privacy	**GPEN publishes report on how privacy enforcement and consumer protection authorities have changed their regulatory and enforcement approaches during COVID-19 and authorities' planned approaches as the pandemic subsides.** • The report highlights that almost half of the 27 authorities responded that they had made changes to their regulatory approach during the pandemic. This was mainly regarding time extensions and many authorities were unsure how to 'revert to their pre-pandemic approach.' • The report notes that some authorities questioned whether there would need to be an 'enhanced' approach in future to strengthen privacy rights as during the pandemic they noted organisations had perceived 'a relaxation of regulatory rules' and there had been a general increase in processing data. ICO report.	Report	New
June 2021	**United Kingdom** Competition and Markets Authority (CMA)	Competition/ anti-trust, consumer protection and privacy	**Mobile ecosystems market study** • The CMA has launched a market study into Apple's and Google's mobile ecosystems over concerns they have market power which is harming users and other businesses. • ICO is engaged in the market study on issues related to Apple & Google's gatekeeper role on App Stores, how that sets privacy standards, whether privacy considerations create restrictions to entry, as well as other aspects.	Market Study and report	New
June 2021	**Norway** Norwegian Consumer Council	Consumer protection and privacy	**Norwegian Consumer Council publishes report on surveillance-based advertising** • The Norwegian Consumer Council published a report, 'Time to Ban Surveillance – Based Advertising: The case against commercial surveillance online,' highlighting the negative consequences these commercial surveillance practices have had on society and consumers.	Report	New

Date	Jurisdiction/s or organisation/s	Area of intersection	Description	Outcome	Status
			• The report lists the negative effects of commercial surveillance as manipulation, discrimination, misinformation, the undermining of competition, security risks and privacy violations. It also provides alternative models, calling on authorities to consider banning the practice. Norwegian Consumer Council press release.		
April 2021	**Philippines** National Privacy Commission	Consumer protection and privacy	**NPC PHE Bulletin No. 18: Online Raffles and Other Games of Chance: Ensuring Proper Safeguards in the Collection of Personal Data** • The NPC urged all businesses, organizations, and individuals who would like to collect personal information for purposes of raffles and giveaways to keep in mind the following practices: • Be more cautious in creating contest mechanics and consider less privacy-intrusive means of collecting personal data. Instead of requiring the public posting of personal data, the mechanics may simply ask participants to like a post, comment an emoji, send a direct message, or other ways that will not necessitate public access to personal data. Data subjects may not be fully aware of, or concerned about, the possible consequences of posting personal data in public platforms. Bulletin.	Guidance	New
2021	**Colombia** Superintendence of Industry and Commerce (SIC)	Consumer protection and privacy	**SIC Case Cooperativa de Ahorro y Crédito Unimos** • In Colombia, sectorial Law 1266 of 2008 regulates the financial and credit information. • A Data subject (consumer) considered that his right has been vulnerated, can file i) a "Acción de Tutela" (numeral 6 of article 16 of said law) or ii) file a complaint in the Superintendence of Industry and Commerce. But cannot file both at the same time. • Every consumer in the Colombian territory that owes money to a company (not a bank) can file a complaint to the DPA if its financial information has been inadequately processed.	Administrative Decision	New
2021	**Colombia** Superintendence of Industry and Commerce (SIC)	Consumer protection and privacy	**SIC Case CIFIN (TransUnion)** • CIFIN added to the credit score of more than 45,835 consumers, information that was prohibited. Apart from publishing the information regarding their debts, the status of political rights suspension was also added. • The Superintendence of Industry and Commerce noted that the suspension of political rights is not information referring to the birth, execution and extinction of monetary obligations referred to in Statutory Law 1266 of 2008. Hence, it is prohibited for CIFIN to add this kind of information.	Administrative Decision	New

Date	Jurisdiction/s or organisation/s	Area of intersection	Description	Outcome	Status
September 2020	**United States** Federal Trade Commission (FTC)	Competition/ anti-trust and privacy	**FTC to hold workshop on data portability** • The FTC will host a public workshop in September 2020 to examine the potential benefits and challenges to consumers and competition raised by data portability. FTC press release.	Public workshop	New
October 2020	**Philippines** National Privacy Commission	Consumer protection and privacy	**NPC Advisory No. 2020-03- Guidelines for Workplaces and Establishments Processing Personal Data for COVID-19 Response** • This Advisory aims to provide additional guidance to supplement the Joint Memorandum CircularNo. 20-04-A Series of 20201 issued by the Department of Trade and Industry and Department of Labor and Employment which requires workplaces and various establishments to collect employee health declaration forms and client/visitor contact tracing forms, and implement measures to manage asymptomatic and symptomatic employees in the workplace. • To ensure the protection of personal data, the Advisory provides for guidance for establishments to adhere to the general data privacy principles of transparency, legitimate purpose, proportionality, implement reasonable and appropriate security measures at each stage of the personal data lifecycle, and uphold data subject rights. Advisory.	Guidance	New
July 2020	**Germany** German competition authority (Bundeskartellamt)	Competition/ anti-trust, consumer protection and privacy	**Bundeskartellamt published its final report into its inquiry into smart TVs** • The Bundeskartellamt has published the final report (in German) on its sector inquiry into smart TVs. The sector inquiry shows that smart TVs can collect personal data in many forms. • The Bundeskartellamt established that almost all smart TV manufacturers active on the German market use privacy policies that have serious shortcomings in terms of transparency and violate GDPR. Bundeskartellamt.	Inquiry and Report	Existing[44]
July 2020	**Philippines** National Privacy Commission	Consumer protection and privacy	**NPC issue Public Health Emergency Bulletin as Guidance for Establishments** • The NPC issued a Public Health Emergency Bulletin as Guidance for Establishments on the Proper Handling of Customer and Visitor Information for Contact Tracing • Pursuant to the Memorandum Circulars of the Department of Trade and Industry (Circular 20-28 s. 2020 and Circular 20-37, s. 2020) on the Guidelines to Follow on Minimum Health Protocols for Establishments, the NPC issued a bulletin to guide	Guidance	Existing[45]

[44] This activity was captured in the DCCWG's 2020 Final Report p. 8.

[45] This activity was captured in the DCCWG's 2020 Final Report p. 2.

Date	Jurisdiction/s or organisation/s	Area of intersection	Description	Outcome	Status
			establishments on the proper handling and protection of personal data collected from customers and visitors. • The bulletin reminds businesses to ensure that processing of personal data is proportional to the purpose of contact tracing, and collect only information required under existing government issuances. • The guidance reiterated that establishments should inform their customers and visitors on the reason for the collection and use personal data only for such declared purpose. • All establishments that collect personal information, whether through physical or electronic means have the obligation to implement reasonable and appropriate safeguards to protect customer data against any accidental or unlawful processing, alteration, disclosure and destruction.		
July 2019-July 2020	**United Kingdom** Competition and Markets Authority (CMA)	Competition/ anti-trust and privacy	**CMA publish a market study on online platforms and digital advertising** • On July 2019, the CMA launched a market study into online platforms and the digital advertising market in the U.K. The CMA assessed three broad potential sources of harm to consumers in connection with the market for digital advertising: o to what extent online platforms have market power in user-facing markets, and what impact this has on consumers o whether consumers are able and willing to control how data about them is used and collected by online platforms o whether competition in the digital advertising market may be distorted by any market power held by platforms. • Following the study, the CMA published its final report on online platforms and digital advertising. The scope of the study includes an assessment of potential sources of consumer harm in digital advertising, including privacy aspects, such as whether consumers are able and willing to control how data about them is used and collected by online platforms. • The study found that Google and Facebook's large user base and access to user data was a source of market power. Privacy aspects are considered in the report. • Amongst other things, the report recommended the introduction of a new pro-competitive regulatory regime for online platforms, including an enforceable code of conduct and the establishment of a new body with powers to make formal interventions such as increasing consumer control over data. The UK government	Market study and Report	Updated[46]

[46] This activity was captured in the DCCWG's 2020 Final Report, pp. 23-24. Updates concerning this activity have since occurred.

Date	Jurisdiction/s or organisation/s	Area of intersection	Description	Outcome	Status
			accepted the findings in the report and set out to create the Digital Markets Unit (DMU) – see above • The ICO was engaged with the CMA on this market study on issues related to the intersection of data protection and competition law.		
July 2020	**United States** Federal Trade Commission (FTC)	Consumer protection and privacy	**FTC to host its fifth annual PrivacyCon 2020** • The FTC announced its fifth PrivacyCon, which will take place on July 21, 2020, an annual event that explores topics related to consumer privacy and security. FTC press release.	Public workshop	Existing[47]
June 2020 – In progress	**Organisations and International Networks** Organisation for Economic Co-operation and Development (OECD) and International Consumer Protection and Enforcement Network (ICPEN)	Consumer protection and privacy	**OECD Consumer Policy Toolkit** • The OECD's Committee on Consumer Policy has developed a Consumer Policy Toolkit. The Toolkit is a practical guide designed to aid policy makers in using a systematic approach to identify and evaluate consumer problems and to develop, implement and review effective consumer policies. OECD press release.	Policy guidance	Existing[48]
March 2020	**Australia** Australian Competition and Consumer Commission (ACCC)	Competition/ anti-trust, consumer protection, and privacy	**ACCC Digital Advertising Services Inquiry** • The ACCC is conducting an inquiry into markets for the supply of digital advertising technology services and digital advertising agency services. • An interim report is due by December 2020. • A final report will be completed by August 2021. ACCC's press release.	Inquiry	Existing[49]
2020	**International networks**	Competition/	**ICN's Project on Competition Law Enforcement at the Intersection of Competition, Consumer Protection and Privacy**	Study	Existing[50]

[47] This activity was captured in the DCCWG's 2020 Final Report p. 22.

[48] This activity was captured in the DCCWG's 2020 Final Report p. 22.

[49] This activity was captured in the DCCWG's 2020 Final Report p. 22.

[50] This activity was captured in the DCCWG's 2020 Final Report p. 23.

Date	Jurisdiction/s or organisation/s	Area of intersection	Description	Outcome	Status
	International Competition Network (ICN)	anti-trust and privacy	• The ICN is a global body committed exclusively to competition law enforcement. Its members represent national and multinational competition authorities. • In its scoping paper, the ICN recognise that competitive markets help achieve the goals of consumer and privacy policies, and enforcing consumer and privacy laws may help make markets become more competitive by enabling consumers to make well-informed decisions about their choices. • The ICN observed complexities and tensions that result from the intersection of regulatory spheres. This includes: o competition and privacy regimes having similar goals to the other, o when applying different regimes, the outcomes may produce tension o issues that present as a competition problem may, on investigation, present consumer or privacy issues, or vice versa o two or more regimes may apply with equivalent, or different results o a finding from one regime may be relevant in another, or the analysis required by another • The ICN observe that the development of data collection/processing practices changes the dynamics of markets, and raises competition law enforcement issues. Recognising the global nature of these issues, the ICN will establish a project that explores the intersection between competition/anti-trust and privacy. ICN Scoping Paper.		
January 2020	**Norway** Norwegian Consumer Council	Consumer protection and privacy	**Norwegian Consumer Council publishes report on ad-tech** • The Norwegian Consumer Council published a report, *'Out of Control: How consumers are exploited by the online advertising industry'* on the current practices of the advertising tech industry, including systematic privacy breaches and unlawful behavioural profiling. • The report focuses on the analysis of data traffic from ten popular apps, such as dating or period tracker apps. It exposes how a large number of mostly unknown third parties receive sensitive and personal data without the knowledge of individuals. Norwegian Consumer Council press release.	Report	Existing[51]
December 2019	**United States** Federal Trade Commission (FTC)	Consumer protection and privacy	**FTC Workshop on Accuracy in Consumer Reporting Workshop** • The FTC, along with the Consumer Financial Protection Bureau, hosted a workshop on accuracy in consumer reporting.	Joint workshop	Existing[52]

[51] This activity was captured in the DCCWG's 2020 Final Report p. 23.

[52] This activity was captured in the DCCWG's 2020 Final Report p. 24.

Date	Jurisdiction/s or organisation/s	Area of intersection	Description	Outcome	Status
	and Consumer Financial Protection Bureau		• The workshop brought together stakeholders—including industry representatives, consumer advocates, and regulators—for a wide-ranging public discussion on the many issues that affect the accuracy of consumer reports. FTC press release.		
October 2019	**European Union** European Commission	Competition/ anti-trust and privacy	**European Commission targeted consultation** • The European Commission undertook a targeted consultation on a draft Communication on the protection of confidential information for the privacy enforcement of EU competition law by national courts. European Commission press release.	Consultation	Existing[53]
October 2019	**United States** Federal Trade Commission (FTC)	Consumer protection and privacy	**FTC Staff Offers Comment on NIST's Proposed Privacy Framework** • The FTC filed a comment on National Institute of Standards and Technology (NIST) proposed privacy framework, which attempts to provide guidance to organizations seeking to manage privacy risks. In the comment, staff of the FTC's Bureau of Consumer Protection commended NIST for proposing a voluntary tool aimed at helping organizations start a dialogue about managing privacy risks within their organizations. The comment suggested certain changes to the proposed framework. FTC press release.	Consultation	Existing
June 2019	**Organisations and international networks** Organisation for Economic Co-operation and Development (OECD)	Competition/ anti-trust, consumer protection and privacy	**OECD discussions** • The OECD has hosted numerous discussions on the intersection of privacy and competition, including: • In June 2019, the OECD hosted the Conference on Competition and the Digital Economy. Discussions were dedicated to Data and competition; digital innovation and competition; and regulatory challenges for competition policy. • In November 2018, the OECD Consumer Protection and Competition committees jointly discussed the ambiguous and multi-dimensional effects of personalised pricing.	Conference	Existing[54]
May 2019	**Organisations and International networks**	Competition/ anti-trust, consumer	**Enforcement Practitioner's Workshop** • The Global Privacy Enforcement Network conducted an Enforcement Practitioner's Workshop in Macau. Representatives from OPC, OAIC, FTC, NPC and the ICO attended.	Workshop	Existing[55]

[53] This activity was captured in the DCCWG's 2020 Final Report p. 24.

[54] This activity was captured in the DCCWG's 2020 Final Report, p. 24.

[55] This activity was captured in the DCCWG's 2020 Final Report, p. 25.

Date	Jurisdiction/s or organisation/s	Area of intersection	Description	Outcome	Status
	Global Privacy Enforcement Network (GPEN)	protection and privacy			
September 2018-June 2019	**United States** Federal Trade Commission (FTC)	Competition/ anti-trust, consumer protection and privacy	**Public Hearings on issues related to Competition and Consumer Protection in the 21st Century** • The FTC held a series of public hearings during the fall 2018 - spring 2019 examining whether broad-based changes in the economy, evolving business practices, new technologies, or international developments might require adjustments to competition and consumer protection law, enforcement priorities, and policy. • Many of the hearings intersected with privacy (Hearing 6 – Privacy, Big Data and Competition; Hearing 9 – Data Security; Hearing 12 – The FTC's Approach to Consumer Privacy).	Public hearing	Existing[56]
March 2019	**United Kingdom** U.K. Digital Competition Expert Panel	Competition/ anti-trust and privacy	**Unlocking digital competition, Report of the Digital Competition Expert Panel** • An independent report on the state of competition in digital markets, with proposals to boost competition and innovation for the benefit of consumers and businesses. • Appointed by the Chancellor in 2018, and chaired by former Chief Economist to President Obama, Professor Jason Furman, the Panel makes recommendations for changes to the U.K.'s competition framework that are needed to face the economic challenges posed by digital markets, in the U.K. and internationally. Their report recommends updating the rules governing merger and antitrust enforcement, as well as proposing a bold set of pro-competition measures to open up digital markets. U.K. Government press release.	Report	Existing[57]
October 2018	**International Network** Global Privacy Assembly (GPA)	Consumer protection and privacy	**Global Privacy Assembly[58] adopts Digital Citizen and Consumer Working Group White Paper** • The DCCWG developed a White Paper which explores the intersection between consumer protection, privacy and data protection as well as other related areas.	Paper	Existing

[56] This activity was captured in the DCCWG's 2020 Final Report, p. 25.

[57] This activity was captured in the DCCWG's 2020 Final Report, p. 29.

[58] The Global Privacy Assembly was known as the International Conference of Data Protection and Privacy Commissioners at this time.

Date	Jurisdiction/s or organisation/s	Area of intersection	Description	Outcome	Status
			Specifically, this report focusses on the procedural and substantive overlaps of these regulatory spheres. • This White Paper was adopted by the Global Privacy Assembly (previously known as the International Conference of Data Protection and Privacy Commissioners).[59] • The White Paper generated further interest and discussions amongst member authorities to explore the intersection of regulatory spheres in further depth and detail, and continue sensitisation in this area.		
2017-2019	**Canada** Competition Bureau (CB)	Competition/ anti-trust, consumer protection and privacy	**Discussion paper considering Big Data and Competition Policy** • In 2017, the Competition Bureau (CB) released its discussion paper 'Big Data and Innovation: Implications for Competition Policy in Canada'. The OPC provided a submission and welcomed the opportunity to engage in a meaningful dialogue with the CB on the challenges relating to the collection, use, and disclosure of personal information in Big Data. • In 2018, the CB released a summary of key themes revealed in its consultation process. In respect of privacy, the CB notes that there are potential overlapping enforcement activities under Canada's competition and privacy law. • In 2019, the CB hosted the Data Forum: Discussing Competition Policy in the Digital Era. Data Portability and the intersection between Privacy and Competition Law were key topics for discussion.	Consultation	Existing[60]

[59] http://globalprivacyassembly.org/wp-content/uploads/2018/11/ICDPPC-DCCWG-Report-Final.pdf.

[60] This activity was captured in the DCCWG's 2020 Final Report, p. 26.

4. Regulatory intersection:
Law and legislative instruments

This table captures instances where laws and legislative instruments address or consider intersection matters or issues. This includes Acts of Parliament, rules and regulations, authorisations, determinations, codes, specifications, orders, notices, and other legislative instruments.

Date	Jurisdiction/s or organisation/s	Area of intersection	Description	Outcome	Status
N/A	**United States** Federal Trade Commission (FTC)	Competition/ anti-trust, consumer protection and privacy	**Federal Trade Commission Regulatory model** • The Federal Trade Commission (FTC) has a unique dual mission to protect consumers and promote competition. The FTC considers privacy through the lens of consumer protection and is an example of where all three regulatory issues intersect.	Co-regulatory model	Existing[61]
2020	**Australia** Office of the Australian Information Commissioner (OAIC) and Australian Competition and Consumer Commission (ACCC)	Competition/ anti-trust, consumer protection and privacy	**ACCC and OAIC Co-regulatory model for data portability scheme in Australia** • Australia is currently developing a national Consumer Data Right (CDR) scheme. • This initiative aims to give consumers greater control over how their data is used and disclosed to create more choice and competition. It is a right to allow consumers to access data in a readily usable form, and to direct a business to securely transfer that data to an accredited third-party data recipient. • The CDR will be rolled out across one sector of the Australian economy at a time. It will commence in the banking sector and will then be implemented in the energy and telecommunication sectors, and finally be rolled out to other sectors over time upon designation by the Treasurer. • Under the legislation, both the OAIC and the ACCC will oversee the CDR under a co-regulator model. The OAIC will regulate the privacy aspects of the scheme, provide	Co-regulatory Data Portability Scheme	Existing[62]

[61] This activity was captured in the DCCWG's 2020 Final Report, p. 28.

[62] This activity was captured in the DCCWG's 2020 Final Report p. 28-29.

Date	Jurisdiction/s or organisation/s	Area of intersection	Description	Outcome	Status
			advice to the ACCC and the Data Standards Body (Data61), and be the primary complaints handler. The ACCC is developing rules and an accreditation scheme to govern the implementation of the CDR and will maintain an "address book" of accredited parties. The OAIC and ACCC will also work closely together to address any systemic breaches of the CDR framework.		