



REGULATING THE DIGITAL ECONOMY – WHY PRIVACY AND COMPETITION AUTHORITIES SHOULD TALK TO EACH OTHER



BY
MELANIE DRAYTON



&
BRENT HOMAN

Acting Deputy Commissioner, Office of the Australian Information Commissioner and Co-chair of the Global Privacy Assembly Digital Citizen and Consumer Working Group.

Deputy Commissioner, Compliance, Office of the Privacy Commissioner of Canada and Co-chair of the Global Privacy Assembly Digital Citizen and Consumer Working Group.

THE FUTURE OF PRIVACY REGULATION

By Kirk J. Nahra



REGULATING THE DIGITAL ECONOMY - WHY PRIVACY AND COMPETITION AUTHORITIES SHOULD TALK TO EACH OTHER

By Melanie Drayton & Brent Homan



THE RIGHT TO PRIVACY AND PERSONAL DATA: SOME CONSIDERATIONS FOR OPTIMAL PROTECTION

By Blanca Lilia Ibarra Cadena



"FIRST ACT" OF THE EUROPEAN DATA ECONOMY - THE DATA GOVERNANCE ACT

By Dr. Paul Voigt & Daniel Tolks



FACEBOOK v. BUNDESKARTELLAMT - MAY EUROPEAN COMPETITION AGENCIES APPLY THE GDPR?

By Anne C. Witt



CAN THE FTC PROMULGATE EFFECTIVE PRIVACY RULES?

By Ben Rossen



THE FTC SAFEGUARDS RULE: INFORMATION SECURITY PROGRAM ELEMENTS

By Melissa J. Krasnow



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

REGULATING THE DIGITAL ECONOMY - WHY PRIVACY AND COMPETITION AUTHORITIES SHOULD TALK TO EACH OTHER

By Melanie Drayton & Brent Homan

Data sits at the center of our digital economy and does not conform to regulatory or geographical boundaries. It is clear further understanding and collaboration by authorities across privacy, consumer protection and competition regulatory spheres is needed to achieve optimal regulatory outcomes. The Digital Citizen and Consumer Working Group ("DCCWG") is focused 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. In doing this, the DCCWG seeks to support "a global regulatory environment with clear and consistently high standards of data protection, as digitalisation continues at pace." This article explores some of the key learnings of the DCCWG over the past 5 years. Ultimately, the DCCWG view is that collaboration between competition agencies and privacy agencies is becoming an imperative for any jurisdiction that seeks to achieve cohesive digital regulation.

Scan to Stay Connected!

Scan here to subscribe to CPI's **FREE** daily newsletter.



01

INTRODUCTION

Data sits at the center of our digital economy and does not conform to regulatory or geographical boundaries. It is clear further understanding and collaboration by authorities across privacy, consumer protection and competition regulatory spheres is needed to achieve optimal regulatory outcomes. In recognition of this, the Global Privacy Assembly established the Digital Citizen and Consumer Working Group (“DCCWG”), which is focused on considering the intersections of, and promoting regulatory co-operation between, the privacy, consumer protection and competition (also referred to as antitrust) regulatory spheres.² In doing this, the DCCWG seeks to support “a global regulatory environment with clear and consistently high standards of data protection, as digitalization continues at pace.”³ This article explores some of the key learnings of the DCCWG over the past 5 years and competitive outcomes.

“Data sits at the center of our digital economy and does not conform to regulatory or geographical boundaries”

The increasing 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, and 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.

Where privacy and consumer protection regulation are more naturally aligned, the same cannot always be said for the privacy and competition regulatory spheres. Accordingly, in recent years, the DCCWG has placed a greater focus on the intersection of privacy and competition in order to better understand how authorities from both regulatory spheres are approaching this intersection and ultimately leverage that understanding in advocating for greater collaboration between competition and privacy regulators. To do so, the DCCWG launched the recently completed privacy and competition “Deep Dive.”

Comprised of two complementary reports, which can be found in the DCCWG’s 2021 Annual Report,⁴ the Deep Dive brings together both the theory and practical application underpinning our current understanding of this intersection. The first is a DCCWG-commissioned independent academic report by Professor Erika Douglas of Temple University Beasley School of Law, titled “*Digital Crossroads: The Intersection of Competition Law and Data Privacy*” (the “Digital Crossroads Report”).⁵ The Digital Crossroads Report is the first of its kind to delve comprehensively into the intersection between competition and privacy. For this report, Douglas reviewed more than 200 publicly available, English-language materials related to antitrust and data privacy agencies around the world. It provides a detailed overview of the current regulatory landscape, highlights compliments and tensions between philosophies at the center of these two regulatory spheres and underlines its emerging development as an important cross-regulatory challenge requiring further consensus-building and international collaboration.

The second is the DCCWG-authored ‘*Privacy and Data Protection as Factors in Competition Regulation: Surveying Competition Regulators to Improve Cross-Regulatory Collaboration*’ (the “Interview Report”).⁶

The Interview Report was based on a series of interviews with competition authorities from around the globe, and identifies key takeaways, potential synchronicity between regulatory spheres as well as obstacles to be surmounted and possible tensions to be mitigated. Perhaps most importantly, the Interview Report also includes multiple practical examples that illustrate how collaboration and communication across regulatory spheres can serve to improve

2 Given the cross-jurisdictional nature of this work, we have used competition and antitrust, as well as “privacy” and “data protection,” interchangeably in this article, while noting of course the terminology is context specific.

3 Global Privacy Assembly, 43rd Closed Session Res, *Strategic Plan 2021-2023* (October 2021), <https://globalprivacyassembly.org/wp-content/uploads/2021/10/2021022-ADOPTED-Resolution-on-the-Assemblys-Strategic-Direction-2021-23.pdf>.

4 Global Privacy Assembly, Digital Citizen and Consumer Working Group, *2021 Annual Report* (August 2021), <https://globalprivacyassembly.org/wp-content/uploads/2021/10/1.3h-version-4.0-Digital-Citizen-and-Consumer-Working-Group-adopted.pdf>.

5 Erika Douglas, *Digital Crossroads: The Intersection of Competition Law and Data Privacy* (Temple University Legal Studies Research Paper No. 2021-40, July 6, 2021), <https://ssrn.com/abstract=3880737> or <http://dx.doi.org/10.2139/ssrn.3880737>.

6 Global Privacy Assembly, Digital Citizen and Consumer Working Group, *supra* note 5, Annex 1.

outcomes for global citizens. Through collaboration there exists an opportunity to leverage cross-regulatory complements and mitigate tensions, and move towards finding a balance without sacrificing the objectives of either regulatory regime. Cross-regulatory collaboration reveals the required synchronization between competition and privacy agencies to support a robust digital economy that engenders consumer trust in privacy protections and competitive markets. In this sense, collaboration between competition agencies and privacy agencies is becoming an imperative for any jurisdiction that seeks to achieve cohesive digital regulation.

With this in mind, this article will explore some of the key findings from those Deep Dive reports, and what this means for the increasing intersection between privacy and competition. This article will first explore both the tensions and shared objectives of these regulatory spheres. It will then outline future opportunities towards a shared understanding. Finally, it will provide some practical insights shared from regulators across the globe, on what it is to co-operate and collaborate across regulatory spheres.

02

TENSIONS AND SHARED OBJECTIVES

As Douglas noted in the Digital Crossroads Report, the interactions between regulatory spheres are nascent, varied and complex. Despite these intersections often being described as complementary, the relationship between antitrust law and privacy is often more nuanced and complex.⁷ Accordingly, Douglas emphasizes the need to bring context to our understanding of how privacy and competition interact with each other as we begin to develop theory, shared understanding, and practice in this area. Recognizing

The first part in building this shared understanding is considering the legal framing of privacy and competition rights and interests, and the different legislative objectives of privacy and competition spheres. Taking this comparative ap-

proach highlighted that both privacy and antitrust/competition law vary by jurisdiction. For example, in the European Union and its member states, data privacy has its foundation as a constitutionally protected right. In contrast, in the United States, data privacy law, at least at the federal level, is a sub-category of consumer protection law. Jurisdictions such as Canada and Australia take a more principles-based approach, rather than conceptualizing privacy in terms of rights.⁸

Furthermore, there is often a different terminology used across jurisdictions. For example, while privacy authorities conceive the term “personal data” as directly relating to protections and sensitivity, competition authorities are more focused on the “data” aspect in the term, particularly in how datasets containing both personal and non-personal data contribute to a company’s market power. This reflection was reinforced by the DCCWG’s Interview Report, where we found that privacy and competition authorities speak different regulatory languages with varied interpretations of certain concepts.⁹

Data protection legislation and antitrust legislation also have different objectives. While data protection law is primarily focused on the privacy interests of individuals, the main objective of antitrust law is to promote economic consumer welfare. As Douglas noted, 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.”¹⁰ The conceptual differences between these regulatory spheres “presents an ‘apples to oranges’ reconciliation between the fundamental human right of privacy, and the economic interests advanced by competition law.”¹¹

Not surprisingly, jurisdictions which are more focused on economic efficiency in their competition law are less likely to incorporate privacy considerations into their competition analysis. On the other hand, jurisdictions which have broader antitrust goals – including fairness and the provision of equitable opportunities for business – have greater scope for including privacy considerations in their competition analysis.¹²

Despite these differences in the objectives between the regimes, there are also common policy interests. For example, both antitrust and privacy law seek to promote consumer trust in digital markets, see data portability as

7 Douglas, *supra* note 6, at 1.

8 *Id.* at 5.

9 Global Privacy Assembly, Digital Citizen and Consumer Working Group, *supra* note 5, Annex 1.

10 Douglas, *supra* note 6, at 31.

11 *Id.* at 33.

12 *Id.* at 6.

beneficial and seek to encourage and maintain consumer choice.¹³ This again points to the value in enhanced collaboration between privacy and competition authorities to work towards these common policy interests.

03

TOWARDS NEW UNDERSTANDING

As identified by Douglas, the current leading theory of the intersection between these areas of law argues that antitrust law should consider privacy only when privacy is a parameter of product (or service) quality that is affected by competition (the “privacy-as quality” theory).¹⁴ The prevalence of the privacy-as-quality theory is illustrated by the fact that it also appears in the Interview Report as the “traditionalist approach to regulation.” Regardless of the name, the central elements of this theory remains the same – privacy will be taken into consideration when it is a competitive factor, and set aside when it is not.

In our (the DCCWG) view, 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 “traditionalist” regulatory approach. While this is arguably an oversimplification, a core tenant of competition theory is that a consolidation of market power increases the likelihood of increased prices which is generally bad for competition. Where privacy is a non-price factor of competition, the inverse likely holds true in that a consolidation of market power increases the likelihood of reduced privacy protections – either because companies no longer feel the need to compete on privacy and reduce their efforts in that area, or because consumers have few privacy related alternatives to choose from – which is bad for privacy.

As the Digital Crossroads Report notes, the implications of the privacy-as-quality theory are still at an early stage, and there are likely to be challenges to its application. For example, how can and should privacy as a non-price factor be

considered in competition analysis? How do competition authorities view privacy harms when they are unrelated to competition? How can the differences in consumer preferences to privacy be accounted for? Because this theory has predominantly been applied to merger reviews, “[i]t 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.”¹⁵ However, as discussed in both the Digital Crossroads Report and the Interview Report, this also represents an opportunity for greater cross-regulatory collaboration in the future. As we (privacy authorities) enjoy a comparative advantage in our understanding of how certain privacy functions operate, we may be able to assist competition authorities improve the level of statistical confidence in their competitive analyses.

For example, privacy authorities are likely to help further the discussion around the concept of the “Privacy Paradox” – which proposes that while individuals claim to value their privacy, their actions suggest otherwise. The idea of the Privacy Paradox complicating efforts to assign a weight to privacy as a non-price competitive factor is discussed at length in the Interview Report. In fact, one of the competition authorities interviewed questioned whether it “might really be a by-product of a corporations’ lack of privacy engagement with individuals, as opposed to the expression of an individual preference (or lack thereof).”¹⁶ While the cause of the Privacy Paradox is up for debate, we (the DCCWG) would suggest that it may be rooted in part in a misunderstanding about what privacy actually means, as some incorrectly equate privacy with secrecy, rather than *control* over one’s personal information, and how/when individuals choose to share it.

Finally, privacy protections are beginning to be cited as a justification for anticompetitive conduct. Both reports analyze the Toronto Real Estate Board’s unsuccessful attempt to cite compliance with Canada’s private sector privacy legislation as a justification for what the courts found to be anti-competitive conduct.¹⁷ As this trend is likely to continue, sharing our privacy expertise will help competition authorities understand whether a company’s actions truly serve a privacy related purpose, whether that company is over-interpreting their privacy obligations, or if they are simply using privacy as an excuse.

This presents a significant opportunity for collaboration between data privacy and antitrust authorities to work to

¹³ *Id.* at 7.

¹⁴ *Id.* at 62-63.

¹⁵ *Id.* at 64.

¹⁶ Global Privacy Assembly, Digital Citizen and Consumer Working Group, *supra* note 5, Annex 1, at 21.

¹⁷ Douglas, *supra* note 6, at 126-130; and Global Privacy Assembly, Digital Citizen and Consumer Working Group, *supra* note 5, Annex 1, at 26 & 27.

develop these analytical tools for measuring the competition-related effects on privacy quality. Accordingly, there is value in deepening that cross-doctrinal understanding and agency cooperation so that enforcement or policy in one area does not unnecessarily undermine the achievements or goals in the other area of enforcement. The shared interests of antitrust and data privacy enforcers can be reinforced to advance their interests.

04

PRACTICAL PERSPECTIVES

Through our ongoing intersection work, as well as the Interview Report, the DCCWG sought to understand how competition authorities are practically approaching privacy and data considerations when carrying out their antitrust analyses, and leverage the views and examples provided in advocating for greater collaboration between competition and privacy regulators. Perhaps most importantly, the Interview Report (a product of interviews with 12 competition authorities around the globe) 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. The benefits of such collaboration are superior outcomes that holistically serve a robust digital economy along with individuals' privacy rights and consumer interests.

The interviews highlighted that there are already many practical examples of regulatory cross-collaboration to date, including:

- i. the creation of cross-regulatory forums (e.g. the UK's *Digital Regulation Cooperation Forum* ("DRCF") and the Australian *Digital Platform Regulators Forum* ("DP-REG")),
- ii. the application of privacy considerations to anti-trust cases (e.g. the German Bundeskartellamt Facebook case, the Competition and Consumer Commission of Singapore's ("CCCS") merger and abuse of dominance guidelines, the United States' Federal Trade

Commission's finding on the Google/DoubleClick merger and the European Commission consideration of the Facebook/WhatsApp merger), and

- iii. the incorporation of privacy considerations into competition remedies (Colombia *Superintendencia de Industria y Comercio* ("SIC") remedy for a banking joint venture).

The UK's DRCF¹⁸ was formed in July 2020 with the overarching goal for participating authorities to better respond to the scale and global nature of large digital platforms and the speed at which they innovate. The DRCF is comprised of the United Kingdom's Competition and Markets Authority, the Information Commissioner's Office, the Office of Communications (or Ofcom) and the Financial Conduct Authority. It is a prime example of how authorities can increase cross-regulatory cooperation, while fulfilling their respective enforcement mandates, via strategic and formalized network engagement.¹⁹

Last month, in March 2022, a collaborative regulator network was established in Australia. The DP-REG' brings together the Australian Communications and Media Authority, the Australian Competition and Consumer Commission, the Office of the Australian Information Commissioner, and the Office of the eSafety Commissioner to support a streamlined and cohesive approach to the regulation of digital platforms.²⁰ This network is an initiative to consider and collaborate around issues of regulating digital platforms with respect to competition, consumer privacy and data regulation, as well focusing on the intersections with online safety issues.

The DCCWG also found that there have been practical examples of applying privacy considerations in competition cases. For example, in the German Bundeskartellamt ("BKartA") Facebook case, BKartA found that Facebook's terms of service, and the manner and extent to which it collects and uses data, amounted to an abuse of dominance. In assessing the appropriateness of Facebook's behavior under competition law, the BKartA took the violation of European data protection rules to the detriment of users into consideration. Where the BKaratA has applied privacy considerations to a single enforcement matter, the CCCS has laid the ground work to apply them to future enforcement matters. As part of a public consultation on proposed amendments to various enforcement guidelines, the CCCS has explicitly stated that, where appropriate, their merger assessments will treat data protection as an

¹⁸ Competition and Markets Authority, The Digital Regulation Cooperation Forum, March 10, 2021 (UK) <https://www.gov.uk/government/collections/the-digital-regulation-cooperation-forum>.

¹⁹ Global Privacy Assembly, Digital Citizen and Consumer Working Group, *supra* note 5, at Annex 1, at 20.

²⁰ Digital Platform Regulators Forum (DP-REG), DP-REG joint public statement, March 11, 2022 <https://www.acma.gov.au/dp-reg-joint-public-statement>.

aspect of quality. Another proposed amendment identified the control/ownership of data as a possible determinant of market power with respect to abuse of dominance assessments.

As a practical example of competition agencies incorporating privacy considerations into their competition remedies, the Interview Report presented the SIC's "Banks" recommendations to the Superintendencia Financiera de Colombia (Colombia's financial regulator) the SIC's T was asked to assess the creation of a new digital joint banking venture. between Colombia's three largest banks It is worth noting that the SIC has multiple enforcement mandates, including consumer protection, privacy and competition. Despite the competitive nature of the assessment, several of the SIC's recommendations were privacy orientated, including ensuring data was treated in compliance with Colombia's privacy laws, obtaining consent, and allowing for data portability.²¹ These practical examples demonstrated the way in which authorities are taking a progressive and proactive approach to considering how privacy and data are factored in antitrust analyses, as the intersection between these two spheres inevitably increases in the digital economy.

05 CONCLUSION

The recent work of the DCCWG, both in commissioning the Digital Crossroads Report and conducting interviews with regulatory authorities resulting in the Interview Report highlighted three consistent key themes.

Firstly, in the digital economy there has been a dramatic expansion in how the privacy and antitrust areas of law interact in digital environments.

Secondly, the theory and understanding in this intersection is still at a very early stage. While there is some emerging consensus, there is still work to be done to build understanding of not only where the intersections are complementary, but where they are not aligned. In this sense, it is essential to deepen our understanding of competition and privacy trade-offs. We need to understand where there are potential trade-offs between the promotion of competition and the protection of privacy in law enforcement and policy, and whether and to what extent such trade-offs are likely to occur.

Thirdly, both of these reports highlight that collaboration between privacy agencies and competition agencies is becoming an imperative for any jurisdiction that seeks to achieve cohesive digital regulation. There are complex questions which need addressing, including how to measure the effects of competition on privacy or vice versa. We need to be asking when and how the quality of privacy protection in a market is likely to be affected by competition. There are many ways in which we can promote cross-regulatory collaboration, including domestic engagement between privacy and competition regulators, participating in global networks for cross-regulatory collaboration and advocating for domestic and international legislative vehicles to remove existing barriers and facilitate cross-regulatory collaboration.

Privacy and competition regulation will continue to intersect, and there will be continued shared goals and areas of tensions as we navigate these spaces. In our research, the DCCWG 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. Regulatory collaboration has the potential to ensure that each regulatory sphere's objectives are advanced. ■

“*Privacy and competition regulation will continue to intersect, and there will be continued shared goals and areas of tensions as we navigate these spaces*”

21 Global Privacy Assembly, Digital Citizen and Consumer Working Group, *supra* note 5, at Annex 1, at 28-29.

CPI SUBSCRIPTIONS

CPI reaches more than **35,000 readers** in over **150 countries** every day. Our online library houses over **23,000 papers**, articles and interviews.

Visit [competitionpolicyinternational.com](https://www.competitionpolicyinternational.com) today to see our available plans and join CPI's global community of antitrust experts.

