
# *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*
21-24 Tirana, Albania

# Contents

FOREWORD ..... 4

EXECUTIVE SUMMARY ..... 5

A. BACKGROUND ..... 5

B. PURPOSE ..... 5

C. WORKING GROUP MEMBERS ..... 6

D. RESOLUTION OBJECTIVES ..... 6

E. ACHIEVEMENTS ..... 7

F. MAPPING OF INITIATIVES CONSIDERING THE INTERSECTION OF PRIVACY, COMPETITION AND CONSUMER PROTECTION ..... 10

G. NEXT STEPS AND RESOLUTION ..... 11

Appendix A: DCCWG White Paper

Appendix B: DCCWG Resolution passed at 40th International Conference

Appendix C: DCCWG Workplan

Appendix D: List of DCCWG Engagements

Appendix E: GPEN Exit Note

Appendix F: DCH Exit Note

Appendix G: Mapping Initiatives

Appendix H: Proposed Resolution

Appendix I: Forward Plan

## Reference table

| **Acronym** | |
|---|---|
| DCCWG | Digital Citizen and Consumer Working Group |
| ICDPPC | International Conference of Data Protection and Privacy Commissioners |
| EDPS | European Data Protection Supervisors |
| FTC | United States Federal Trade Commission |
| ICO | Information Commissioner's Office, United Kingdom |
| NPC | National Privacy Commission, Philippines |
| OAIC | Office of the Australian Information Commissioner |
| OPC | Office of the Privacy Commissioner of Canada |
| ICPEN | International Consumer Protection and Enforcement Network |
| GPEN | Global Privacy Enforcement Network |
| DCH | Digital Clearinghouse |
| CPC Network | European Consumer Protection Cooperation Network |
| APPA | Asia Pacific Privacy Authorities |
| DPA | Data Protection and Privacy Authorities |
| MOU | Memorandum of Understanding |

## FOREWORD

As co-chairs of the Digital Citizen and Consumer Working Group (DCCWG), we are pleased to present this report to the 41st *International Conference of Data Protection and Privacy Commissioners* in Tirana, Albania.

This report provides an overview of the DCCWG's inception and objectives, and represents the work the DCCWG has completed over the past 12 months. This report also outlines next steps for the DCCWG, as detailed in its proposed resolution, to be presented at the 41st International Conference, and 'forward work plan' for the coming two years.

All attendees of the Tirana Conference are warmly invited and encouraged to take note of this report and the proposed Draft Resolution, and to consider co-sponsoring the Resolution. Should any questions arise about this report or the work done by the Working Group, the co-chairs remain available for queries.

Finally, the co-chairs would like to thank all the members of the Working Group for their active involvement in, and continued engagement with the Working Group, as well as for their invaluable input and contributions that led to fruitful discussions and new insights.

| | |
|---|---|
| *Co-Chair* | *Co-Chair* |
| Office of the Privacy Commissioner of Canada | Office of the Australian Information Commissioner |

## EXECUTIVE SUMMARY

The work of the DCCWG over the past 12 months has identified that in many jurisdictions, there have been substantive initiatives that have increased collaboration and co-operation between Data Protection and Privacy Authorities and Competition or Consumer Authorities. These have ranged from policy initiatives such as the Philippines' Development of advisories and papers on the protection of personal information of digital consumers, to Government Inquiries, such as Australia's Inquiry into Digital Platforms, which considered these organisations' collection, use and disclosure of personal information and the need for consumer protection.

However, from the DCCWG's work on engaging with various international fora, it is evident that these are still early days for the examination and full appreciation of the intersection phenomenon. As such, the DCCWG's work on mapping the intersection of legislation and policy across sectors, and the sensitization of authorities to those intersections, continues to be a cornerstone of the DCCWG's objectives.

Notwithstanding the above, the DCCWG recognizes that while certain jurisdictions are in the nascent stages of cross-regulatory cooperation, there are others where collaboration is already occurring. Therefore, in its proposed forward work plan, the DCCWG has outlined how it intends to provide opportunities to concert efforts towards developing avenues for cooperation and collaboration between regulatory spheres.

## A. BACKGROUND

1. The *Digital Citizen and Consumer Working Group* ("DCCWG") studies the intersections between privacy/data protection, and consumer protection and competition. The working group, which was established via a resolution passed at the 39th *International Conference of Data Protection and Privacy Commissioners* ("ICDPPC" or "International Conference"), authored a 'white paper' on the subject (Appendix A), which it presented at the 40th International Conference. At that conference, a second resolution was passed to renew and confirm the mandate of the DCCWG, to continue the study of these intersections (Appendix B). Subsequently, the DCCWG set out a work plan (Appendix C) for the 2018-2019 period.

## B. PURPOSE

2. The purpose of this report is to inform the ICDPPC of the work undertaken by the DCCWG over the 2018-2019 year, and to update members on the status of the objectives set out in the second resolution.

3. This report also provides details on the proposed future direction of the DCCWG and seeks a renewed mandate for the 2019-2021 period.

## C. WORKING GROUP MEMBERS

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

- Authority for Consumer & Markets – Netherlands (observer)
- Belgian Data Protection Authority ("Belgium DPA")
- Datatilsynet Norway
- Datatilsynet Denmark
- European Data Protection Supervisor ("EDPS")
- United States Federal Trade Commission ("FTC")
- Information Commissioner's Office, United Kingdom ("ICO")
- National Privacy Commission, Philippines ("NPC")
- Office of the Australian Information Commissioner ("OAIC") (co-chair)
- Office of the Privacy Commissioner of Canada ("OPC") (co-chair)

## D. RESOLUTION OBJECTIVES

5. The 2018-2019 resolution, passed at the 40th International Conference, resolved to:

a) continue efforts to bring about effective inter-and intra-jurisdictional cooperation between data protection and consumer protection authorities in specific cases or categories of cases to improve outcomes for individuals' rights;

b) consider the interaction of privacy / data protection regulation and competition, and the implications for consumers;

c) continue to study the overlap of substantive legislation affecting the rights of digital consumers;

d) increase the presence of the DCCWG at international fora that consider the intersection between privacy and data protection, including the *International Consumer Protection and Enforcement Network* (ICPEN), the *Global Privacy Enforcement Network* (GPEN), the *Digital Clearinghouse* (DCH), and the *Consumer Protection Cooperation Network* (CPC Network); and

e) leverage this presence to engage authorities responsible for consumer, privacy and data protection, as well as other relevant authorities, such as competition and antitrust enforcement authorities, in an effort to monitor and map relevant enforcement cases and jurisprudence affecting the privacy of digital consumers, for example, in order to better understand how to design multi-disciplinary approaches to statutory protections for individuals' data.

## E. ACHIEVEMENTS

6. The DCCWG met all of its resolution commitments.

7. Throughout the 2018-2019 year, the DCCWG has continued efforts to bring about effective cooperation among regulators by raising awareness of cross-regulatory intersections and sharing information about these intersections with various networks of global reach. We have actively pursued engagement with various international fora, and have conducted several presentations on the white paper. In particular, DCCWG members have conducted presentations at conferences hosted by the *Asia Pacific Privacy Authorities* ("APPA"), GPEN, the CPC Network and the DCH. See Appendix D for a complete list of engagements.

8. A key goal for the past year was to arrange a workshop that would allow for the identification of strategies and best practices for collaboration among Data Protection and Privacy Authorities (DPAs) and consumer protection and/or competition authorities. The main objectives of the workshop were to: gain a better understanding of how to design multi-disciplinary approaches to statutory protections for individuals; and, hear from authorities about their experiences with the intersection, including when their mandate has overlapped or intersected with that of another cross-sectoral regulator.

9. The Working Group leveraged two events under this workstream: (i) a collaborative initiative with GPEN, and (ii) participation at the DCH.

### *DCCWG – GPEN Workshop*

10. At the GPEN Enforcement Practitioners Workshop (Macao, China) in May of this year, the DCCWG led a co-branded session on the intersection between privacy, consumer protection and competition, which consisted of a brief presentation followed by a structured breakout session (workshop) where participants were divided into groups to share their experiences with cross-disciplinary collaboration. In order to encourage focussed dialogue amongst participants, questions on cross-disciplinary collaboration were provided in advance of, and during, the conference. In particular, we sought examples of lessons learned from experience

with such collaboration – i.e., best practices, challenges or key takeaways that would help us further explore this topic, and feed back into the ICDPPC membership.

11. The breakout session/workshop led to substantive contributions on the topic, received positive feedback from participants, and furthered our exploration of how DPAs are collaborating with consumer and competition agencies (and other regulators such as cybercrime authorities). An Exit Note (Appendix E), consisting of takeaways from the sessions, was then prepared and shared with the GPEN network.

12. A sampling of the strategies/tools/experiences identified include:

- Most DPAs indicated that they were cooperating with their consumer protection regulators on a policy level (through joint publications, training or mutual participation in public consultation) – some had concluded Memoranda of Understanding (MOUs) and others had not;

- One jurisdiction's government had proposed legislation surrounding data portability that would make both the consumer regulator and privacy regulator responsible for implementation;

- In terms of the intersection between privacy and competition, most authorities indicated that the building of connections was still in its primary stages – we did however see a range of answers:

    - Some DPAs mentioned ad hoc interaction with their competition authority;

    - We saw DPAs arranging training with their competition authority to enhance cross-agency knowledge of the law; and

    - Others indicated that high-level meetings between Commissioners are occurring.

- We also heard that the practical and experiential aspect of the intersection between competition and privacy needs further exploration, for example, to gain an understanding of how privacy is considered when a high profile merger involving personal data is taking place;

- We also heard that many legal issues also relevant to privacy arise where competition cases involve technology (e.g., mergers of tech companies with personal data as assets);

- Almost across the board, the inability to share information was cited as a barrier to cooperation – in particular, where this information was subject to secrecy, confidentiality or commercially sensitive provisions. Some participants stated that a legal amendment would be required to allow for cross-regulatory information sharing in their jurisdiction; and

- One key takeaway related to timing – problems can arise when one authority announces the opening or outcomes of a case while a related investigation is still ongoing for a cross-regulatory counterpart. Participants suggested that a good practice may be to agree, at the start of an investigation, on whether each agency will be informing the other of likely timelines for outcomes, or providing a 'heads up' to facilitate potential shared communications strategies.

13. Furthermore, certain good practices were cited:

- Consult where there is overlap, in order to establish a mutual trust between regulators;

- Have a designated point of contact in each agency and maintain routine communication – enable an ease of doing business such that you can pick up the phone to call your contact;

- Ensure all regulatory issues are identified and dealt with by the regulator with the appropriate expertise, with input from others as required;

- Put in place information sharing agreements or MOUs;

- Advocate for information sharing authorization in each agency's legislation to ensure that expertise and complaint/enforcement information can be shared; and

- Identify challenges and hurdles in areas of overlap, and learning from experience, implement measures to overcome those.

14. Lastly, the DCCWG leveraged working group members' participation at the Workshop by drawing upon its members - representatives from the FTC, ICO, NPC, OAIC, and OPC - to help lead structured discussions during the breakout session, which were yielded the lessons learned captured in the DCCWG-GPEN Exit Note.

***Digital Clearing House (DCH)***

15. The DCCWG also sought to hold a similar workshop as part of the DCH meeting that took place on June 5th, 2019 in Brussels.

16. The DCH brings together agencies that oversee legislation that regulates the digital economy, in particular both competition and privacy authorities, in order to discuss the intersections between privacy and competition. The June 5th DCH meeting focussed on whether and how privacy can be considered as a part of an antitrust case, for example, by considering privacy as a non-price effect of a merger. At that meeting, the DCCWG presented highlights from the GPEN session and requested that attendees of the DCH provide examples of best practices, challenges or key takeaways stemming from their experiences with the intersection. We received several written responses to the questions, and the DCH discussion was lively and positive, with the meeting host highlighting the importance and relevance of the DCCWG efforts, requesting a dedicated session at the DCH meeting post the 41st ICDPPC in Albania. Appendix F contains a summary of the responses to questions received from DCH participants.

## F. MAPPING OF INITIATIVES CONSIDERING THE INTERSECTION OF PRIVACY, COMPETITION AND CONSUMER PROTECTION

17. DCCWG members continue to monitor intersecting enforcement cases, policy projects and/or academic articles involving the interaction between privacy and data protection, and consumer protection or competition. Appendix G captures some of the initiatives, from around the world, that are considering the intersection of privacy and competition or consumer protection. While the table does not include an exhaustive list of such initiatives, it does show the development of governments' and regulators' work in the intersection sphere across regions, including in relation to: policy considerations, laws and legal instruments, and enforcement actions.

18. *Policy considerations*
There have been policy developments occurring across the globe, including in the US, Canada, Australia, Singapore and Europe. In some instances, we have seen these discussions progress into Government Inquiries.

Separately, we have seen an academic journal devoted mainly to competition analysis include an article on privacy issues, and an international privacy law journal devote an entire issue to competition.

19. *Developments with respect to laws and legal instruments*
In certain jurisdictions, we are seeing proposed legislation which has a dual role for the Competition and Data Protection regulators.

20. *Enforcement actions*
    In other jurisdictions, we are seeing cases where competition regulators are relying on data protection legislation to prosecute. There have been notable cases in this area, including the German Facebook case as the landmark example. We have also seen consumer protection authorities pursuing actions with respect to obtaining consent for the collection and use of personal data. Finally, we noted cooperation occurring between the enforcement networks ICPEN and GPEN, surrounding terms and conditions in the digital economy, and the GPEN endorsement of an ICPEN letter to App marketplaces.

21. Each of these initiatives has been mapped in Appendix G.

## G. NEXT STEPS AND RESOLUTION

22. While we continue to see collaborative efforts, within international regulatory fora, to better understand and map out these intersections, we still view this work as just beginning. The importance and present day relevance of this work is now evidence-based, as business or regulatory decisions in one field have started affecting other regulatory fields. We have seen an expanded interest in intersecting issues since the inception of the DCCWG, which has proved prophetic and validating. Our long-term goals for the DCCWG include advancing the will, and realizing the mechanisms, to collaborate with enforcement partners across regulatory spheres, with a view to having holistic and efficient regulatory outcomes that provide a greater scope of coverage for consumers from privacy, consumer protection and competition risks. To this end, the Working Group has submitted a resolution to the 41st International Conference for the ICDPPC's consideration and adoption.

23. The DCCWG is proposing a resolution that will extend the working group's mandate for a duration of two (2) years. The proposed resolution is included at Appendix H.

24. The DCCWG's forward work plan is included at Appendix I.

# Appendix A: DCCWG White Paper

# ICDPPC Digital Citizen and Consumer Working Group

Report to the 40th Conference on the collaboration
between Data Protection, Consumer Protection and other Authorities for Better Protection of Citizens and Consumers in the Digital Economy

## Table of Contents

Introduction ..... 3
CHAPTER I ..... 4
Why look at the intersection of privacy and consumer protection: Consumer relationships are data relationships ..... 4
Consumer Protection and Data Protection ..... 5
Exploring the Intersection ..... 6
Deceptive Marketing Practices and Lack of Consent ..... 6
Terms and Conditions ..... 8
Harmful or Inappropriate Uses of Personal Information ..... 9
Privacy Protection and Competition ..... 11
CHAPTER 2 ..... 14
Identifying and fostering (inter)national collaboration initiatives ..... 14
National collaboration initiatives ..... 14
The smart watches case - co-operation between data and consumer protection authorities in Norway 15
Dutch collaboration agreement between the data protection and consumer protection authority ..... 16
International collaboration initiatives ..... 17
The Global Privacy Enforcement Network's Network of Networks Initiative ..... 17
OECD Recommendation on Cross-border Co-operation in the Enforcement of Laws Protecting Privacy. 18
GPEN practitioner's event ..... 19
Digital Clearinghouse ..... 19
Collaboration mechanisms ..... 20
Secondments / Staff Exchanges / Fellowships ..... 20
Referrals ..... 21
Regional collaboration mechanisms (an EU example) ..... 22
CHAPTER 3 ..... 25
Substantive Challenges and Overlaps ..... 25
Fairness ..... 25
Consent as a common issue ..... 29
CHAPTER 4 ..... 33
Further action of the Working Group ..... 33

# Introduction

1. The 39th *International Conference of Data Protection and Privacy Commissioners* ("ICDPPC"), passed a resolution regarding collaboration between Data Protection Authorities and Consumer Protection Authorities towards better protecting citizens and consumers in the digital economy.[1]

2. The ICDPPC resolution established the *Digital Citizen and Consumer Working Group* ("Working Group"). The resolution tasked the Working Group with identifying, leveraging and building upon existing initiatives and networks that consider the intersection between consumer, data and privacy protection, and exploring how authorities may use existing legislative frameworks to work together and secure better data protection outcomes for citizens and consumers.

3. The Working Group submits this report that explores the intersection between consumer protection, privacy and data protection as well as other related areas. Specifically, this report focusses on the procedural and substantive overlaps of these regulatory spheres.

4. This report is comprised of four main chapters. **Chapter I**, "Why look at the intersection of privacy and consumer protection," introduces the intersections between consumer protection, data protection and competition concepts. **Chapter II,** "Identifying and fostering (inter)national collaboration initiatives," identifies existing international fora which allow the exchange of experiences and best practices between agencies. It highlights examples of inter-agency collaboration on a national level and brings forward suggestions and mechanisms for cooperation on national and international levels. **Chapter III,** "Substantive challenges and overlaps," discusses the substantive overlaps and common ideals shared between the regulatory spheres such as fairness, transparency and consent. **Chapter IV**, "Recommendations," recommends further work to be undertaken by the Working Group.

[1]ICDPPC, "Resolution on Collaboration between Data Protection Authorities and Consumer Protection Authorities for Better Protection of Citizens and Consumers in the Digital Economy", 26-27th September 2017, Hong Kong, link.

# CHAPTER I

## Why look at the intersection of privacy and consumer protection: Consumer relationships are data relationships

1. Individuals' ordinary daily activities are increasingly sharing a particular characteristic: they are generating the data that fuels the digital economy. Business models continue to rapidly evolve, in part due to advanced algorithms, artificial intelligence, and predictive analytics, all of which give organisations the ability to calculate, analyse, and make inferences with large volumes of data at a high velocity.

2. As more data is gathered about consumers over longer periods of time, individuals' habits and patterns become more evident to businesses. To this end, consumer relationships in the digital economy have also evolved into data harvesting relationships. As databases and analytics capabilities grow, even relatively small businesses can obtain granular details about individuals – including but not limited to their purchases, behaviours, locations and interests.

3. Individuals are increasingly aware of the role their personal information plays in the digital economy – but may not necessarily be aware of the full extent of all the ways their information is used. As a result, there are concerns as to how personal information is processed, whether and how individuals can assert control over their information, and the scale and scope of information being amassed by organizations in the digital environment.

4. Issues related to data being collected and used in the digital economy are becoming an area of increasing interest not only for privacy regulators, but also for regulators in consumer protection. Harmful, deceptive, or misleading privacy practices can result in situations that raise concerns and lead to enforcement action under both privacy and consumer protection legislation.

5. The challenges raised by the fusing of consumer relationships with data relationships has led to discussions as to whether there is a need for enforcement authorities in consumer protection and privacy to explore the benefits of a co-operative and collaborative framework to the application of their laws. By examining the intersection of these two areas, regulators can better understand where principles converge and diverge, how each authority can support common objectives, mitigate regulatory ambiguity, and develop best practices that result in positive outcomes for both digital citizens and consumers.

6. Given the importance of personal information in the digital economy, and the increasing degree to which consumer relationships are becoming data relationships, some regulators have begun to raise questions regarding the interplay of antitrust,

competition, consumer protection, data protection and privacy. For example, EU data protection authorities have recently raised the point that "*increased market concentration in digital markets has the potential to threaten the level of data protection and freedom enjoyed by consumers of digital services*"[2]. They considered it essential to assess the longer-term implications of economic concentrations in the digital economy on data protection and consumer rights[3]. This report does not examine these broader issues, but rather, focuses primarily on the conceptual and legislative overlap between consumer protection and data protection.

## Consumer Protection and Data Protection

7. Consumer protection is rooted in the need to promote informed consumer decision-making and to protect consumers from deception, unfair practices, and unsafe products that cause detriment or harm.[4] Often such detriment is the consequence of a lack of information on the consumer side. As stressed in the OECD Consumer Policy Kit (2010), addressing market failures that arises out of a lack of information is a primary focus of consumer protection legislation.[5]

8. As emphasised in the OECD Privacy Guidelines (2013), privacy and data protection legislation also introduce transparency obligations vis-à-vis data subjects as a means to hold organizations accountable for their data processing operations. The guidelines recognize that questions on the effectiveness of consumer's choice based on the level of information provided to them are also instructive in the area of privacy protection[6].

9. In its paper titled: *Big data and Innovation: Implications for Competition Policy in Canada*[7], the Competition Bureau of Canada makes some particularly pertinent remarks on the intersection between consumer protection and privacy, indicating that the mandates of both the Canadian Competition Bureau and the Office of the Privacy Commissioner of Canada ("OPC") may overlap in this area:

> *There is potential for overlapping enforcement activities under the [Competition] Act and under privacy law. Canada's Office of the Privacy Commissioner (OPC) has a mandate under the Personal Information Protection and Electronic Documents Act (PIPEDA) to protect and promote privacy rights in the collection,*

[2] EDPB, "Statement on the data protection impacts of economic concentration", 27 August 2018, link.
[3] Ibid.
[4] OECD, "Recommendation on consumer policy decision making", 2014, link.
[5] OECD, "Consumer Policy Kit", 2010, pg. 32, link.
[6] OECD, "The OECD Privacy Framework", 2013, pg. 99, link.
[7] COMPETITION BUREAU CANADA, "Big data and innovation: key themes for competition policy in Canada", 19 February 2018, link.

> *use, and disclosure of personal information. One principle holds that PIPEDA "is intended to prevent organizations from collecting information by misleading or deceiving individuals about the purpose for which information is being collected." Similarly, the [Competition] Act condemns representations made to the public that are false or misleading in a material respect.* ***Therefore, the Bureau's mandate to ensure truth in advertising may overlap with the OPC's mandate to protect privacy rights. Both mandates are important to protect consumers in the digital economy.***"[8] (emphasis added)

10. Ultimately, consumer, data, and privacy protection frameworks share a common ground of aiming to protect individuals — consumers or data subjects — from harm due to deception, manipulation or misuse. Through the promotion of honesty and transparency, consumer protection and privacy frameworks can help to confer greater control to individuals.

## Exploring the Intersection

11. Three examples of where there has been overlap between the areas of consumer protection and privacy include: *Deceptive Marketing Practices and Lack of Consent*, *Terms and Conditions*, and *Harmful or Inappropriate Uses of Personal Information* (discussed further below). These examples highlight real world cases where the legal frameworks governing consumer, data, and privacy protection may overlap.

### Deceptive Marketing Practices and Lack of Consent

12. The digital economy recognizes that personal data has increased in both value and volume, and fraudsters and miscreants have taken notice that personal data has become a form of currency such that the growth of personal information accessible online has incentivized wrongdoers to find ways to exploit it.

13. The increased concern over how information is being used and protected by businesses is shared by consumers, who value their privacy. In short, privacy and security have now become material considerations that can inform and influence consumers' purchasing decisions. Because of this, businesses market privacy in their products or services.

14. For example, in the international investigation of AshleyMadison.com[9] the company was found to be marketing privacy in a deceptive manner. AshleyMadison.com advertised itself as a "100% discreet service" for people seeking to have affairs, and bolstered that claim with a security "trustmark" icon, or "trusted security award". The investigation found the "trustmark" was a complete

[8] Ibid.

[9] The joint investigation was carried out between the Australian Office of the Information and Privacy Commissioner, US FTC, and the Office of the Privacy Commissioner of Canada.

fabrication and secured its removal. The investigation also revealed that the company offered a deceptive "full delete" feature for an extra charge. Users who chose this option, however, would have not known that their profile information was not deleted, instead retained for up to one year after paying for a "full delete".

15. In a similar vein, an Internet-based operation that finds potential borrowers for mortgage refinancing lenders had settled with the United States Federal Trade Commission ("US FTC") after having deceived consumers with ads falsely claiming they could refinance their mortgages for free.[10] Consumers following the ads were sent to a landing page where they voluntarily provided contact information, which was ultimately passed on to providers of mortgage refinancing.

16. Traditionally it is the mandate of consumer protection authorities to enforce prohibitions of deceptive marketing practices, such as false or misleading representations made to the public for a commercial purpose. For example, in Canada sections 74.01(1) and 52(1) of Canada's *Competition Act* states that no person shall make/a person engages in reviewable conduct when a representation is made to the public that is false or misleading in a material respect, for the purpose of the promotion or supply of a product:

> *"**False or misleading representations***
>
> ***52 (1)** No person shall, for the purpose of promoting, directly or indirectly, the supply or use of a product or for the purpose of promoting, directly or indirectly, any business interest, by any means whatever, knowingly or recklessly make a representation to the public that is false or misleading in a material respect. (Criminal provision)*
>
> ***Deceptive Marketing Practices***
>
> ***74.01 (1)** A person engages in reviewable conduct who, for the purpose of promoting, directly or indirectly, the supply or use of a product or for the purpose of promoting, directly or indirectly, any business interest, by any means whatever, makes a representation to the public that is false or misleading in a material respect; (Civil provision)"* [11].

Also under privacy legislation, consent cannot be obtained through deception. To make consent meaningful, privacy legislation requires organisations to state the purposes for which the information will be used so that consumers can reasonably understand how their information will be collected, used or disclosed. Simply put, an individual cannot meaningfully consent to a lie.

17. For example, in Canada, principles 4.3.5 and 4.4.2 of the *Personal Information Protection and Electronic Documents Act* (PIPEDA) states that consent with

[10] FTC, "Mortgage Lead Generator Will Pay $500,000 to Settle FTC Charges That It Deceptively Advertised Mortgage Refinancing", 12 September 2014, link.
[11] *Competition Act*, R.S.C., 1985, c. C-34, link.

respect to the collection, use or disclosure of personal information must not be obtained through deception:

> *"**Principle 3 – Consent***
>
> *4.3.5. In obtaining consent, the reasonable expectations of the individual are also relevant. For example, an individual buying a subscription to a magazine should reasonably expect that the organization, in addition to using the individual's name and address for mailing and billing purposes, would also contact the person to solicit the renewal of the subscription. In this case, the organization can assume that the individual's request constitutes consent for specific purposes. On the other hand, an individual would not reasonably expect that personal information given to a health-care professional would be given to a company selling health-care products, unless consent were obtained.* ***Consent shall not be obtained through deception.*** *[Emphasis added]*
>
> ***4.4 Principle 4 — Limiting Collection***
>
> *The requirement that personal information be collected by fair and lawful means is intended to prevent organizations from collecting information by misleading or deceiving individuals about the purpose for which information is being collected.* ***This requirement implies that consent with respect to collection must not be obtained through deception.*** *[Emphasis added]."* [12]

18. Given the above, in Canada, *both* the Competition Act and PIPEDA could address a circumstance where an organization, in the course of supplying or promoting a product obtains consent for collection, use or disclosure of personal information, but the consent in question was obtained via false, misleading, or deceptive means.[13]

## Terms and Conditions

19. Digital citizens and consumers seeking to engage in digital economy are regularly confronted with terms and conditions that purport to outline the privacy implications of the collection of their personal information. Consumer protection and privacy may intersect where consumers are asked to accept terms and conditions which may lack transparency, contain hidden material elements notably on the use of data, and/or contradict the general impression conveyed by more prominent messaging.

20. The last point represents a key tenet of consumer protection legislation - individuals should not be misled by general impression of the product. For example, if a product is advertised as "privacy friendly", its terms and conditions that contradict the general impression that the product is "privacy friendly" could be deceptive.

---

[12] *Personal Information Protection and Electronic Documents Act*, S.C. 2000, c. 5, link.

[13] Furthermore, Canada's Anti-Spam legislation ("CASL") is enforced by three federal authorities, including the Office of the Privacy Commissioner of Canada, the Competition Bureau Canada, and the Canadian Radio-television and Telecommunications Commission.

Privacy legislation requires businesses to be transparent about privacy and disclose the purposes for which personal information will be used. Under both consumer protection and privacy law, terms and conditions should not result in misleading consumers about the collection of their personal information.

21. In a real-world example, the US FTC charged the creator of a popular flashlight app for Android mobile devices, for deceiving consumers about how their geolocation information would be shared with advertising networks and other third parties (the app developer settled the matter with the US FTC).[14] In that case, the company's privacy policy did not adequately disclose to consumers that the app transmitted device data, including precise geolocation and persistent device identifiers to third parties, including advertising networks. Self-evidently, there is no meaningful link between a flashlight function on the one hand and the processing of location data on the other. Under a privacy approach: an organisation would *only* collect, use and disclosure information for a *legitimate* and identified purpose, would give appropriate notice of this collection, and would potentially face stricter consent requirements when precise geolocation information was at issue.

22. The International Consumer Protection and Enforcement Network (ICPEN) is also acting on the topic of terms and conditions and launched an appeal to all businesses in the digital economy to review these[15]. After a coordinated sweep action in February 2018 the participating ICPEN members identified a number of concerns with terms and conditions such as these being lengthy, too hard to understand, containing hidden information and failure to respect statutory consumer and privacy rights. The open letter sent by the ICPEN presidency highlights a number of best practices in an attempt to encourage businesses to review their terms and conditions.

## Harmful or Inappropriate Uses of Personal Information

23. Consumer protection and privacy protection may also intersect when personal information is posted online for an inappropriate purpose. For example, mugshots taken of individuals while arrested have been disseminated by companies online, without the knowledge or consent of the individual in the mugshot, and can be easily found via popular search engines.[16] Certain websites hosting this personal information operate a "pay for takedown" scheme—a scam where a website posts, or facilitates the posting of, defamatory, inflammatory, or embarrassing

[14] FTC, "Android Flashlight App Developer Settles FTC Charges It Deceived Consumers", 5 december 2013, link.
[15] ICPEN, "Joint open letter to businesses in the digital economy on the importance of standard terms and conditions for consumers", 29 June 2018, link.
[16] PEW, "Fight against mugshot sites brings little success", December 11th 2017, link.

information, in order to extort people who have an incentive to pay to have that information taken down.[17]

24. Such a scheme has been thwarted recently in the US. Four individuals were charged with extortion, money laundering, and identity theft for allegedly running the website Mugshots.com.[18] The allegations include using personal information (names, police booking photos, charges against the individual) for the purpose of charging a "de-publishing fee" to have the content removed. The State of California Department of Justice stated:

> "*The website mines data from police and sheriffs' department websites to collect individuals' names, booking photos and charges, then republishes the information online without the individuals' knowledge or consent. Once subjects request that their booking photos be removed, they are routed to a secondary website called Unpublisharrest.com and charged a "de-publishing" fee to have the content removed. Mugshots.com does not remove criminal record information until a subject pays the fee. This is the case even if the subject had charges dismissed or had been arrested due to mistaken identity or law enforcement error. Those subjects who cannot pay the fee may subsequently be denied housing, employment, or other opportunities because their booking photo is readily available on the internet.*"[19]

25. In another example, an investigation by the OPC into Globe24h.com ("Globe24") looked into the company's practice of re-publishing legal decisions in a way that made those decisions discoverable by searching an individual's name in a popular search engine.[20] For example, if an individual was involved in bankruptcy proceedings, custody matters or labour relations matters, and someone searched that individual's name on a search engine, the legal decision involving that person would show up on Globe24 in the search results. In order for an individual to have the link removed, Globe24 required the individual to pay a fee. The OPC found that Globe24 was operating a "pay-for-takedown" scheme, concluding that Globe24 was collecting, using and disclosing personal information for an inappropriate purpose and filed an application in Federal Court to enforce its decision. The Canadian Federal Court declared that personal information was being used for an inappropriate purpose and ordered the operator of the website to remove all Canadian court and tribunal decisions containing personal information, as well as

[17] Often such schemes do not follow through on the "takedown" portion of the play, rather payers are marked as easy targets to perpetuate the scam.
[18] STATE *OF* CALIFORNIA DEPARTMENT *OF* JUSTICE, "Attorney General Becerra Announces Criminal Charges Against Four Individuals Behind Cyber Exploitation Website", Press release, 16 May 2018, link.
[19] Ibid.
[20] OPC, "Website that generates revenue by republishing Canadian court decisions and allowing them to be indexed by search engines contravened PIPEDA", 5 June 2015, link.

taking the necessary steps to remove the decisions from search engine caches. Damages of $5,000 were awarded to the complainant.[21]

26. Yet another example of the intersection between privacy and consumer protection can be found in recent enforcement by the US FTC against data broker LeapLab.[22] The US FTC alleged that LeapLab bought payday loan applications and then sold the information found in those applications to marketers whom LeapLab knew had no legitimate need. At least one of those marketers allegedly used the information to withdraw millions of dollars from consumers' accounts without their authorization. Here the unauthorized disclosure of personal information by LeapLab to someone without a legitimate need was a key step in the perpetration of fraud.

## Privacy Protection and Competition

27. As personal information is increasingly a component of business models and business transactions, competition enforcement authorities are beginning to explore the implications of personal information and privacy within their analytical frameworks.

28. For example, the German and French competition authorities wrote a joint report on the role of data in economic relationships as well as in the application of competition law to such relationships. In this report they identified some intersections between data protection and competition law:

> *"Indeed, even if data protection and competition laws serve different goals, privacy issues cannot be excluded from consideration under competition law simply by virtue of their nature. Decisions taken by an undertaking regarding the collection and use of personal data can have, in parallel, implications on economic and competition dimensions. Therefore, privacy policies could be considered from a competition standpoint whenever these policies are liable to affect competition, notably when they are implemented by a dominant undertaking for which data serves as a main input of its products or services. In those cases, there may be a close link between the dominance of the company, its data collection processes and competition on the relevant markets, which could justify the consideration of privacy policies and regulations in competition proceedings".*[23]

[21] FEDERAL COURT (Canada), *AT v. Globe24h.com and Sebastian Radulescu*, 30 January 2017, link.
[22] FTC, "FTC Charges Data Broker with Facilitating the Theft of Millions of Dollars from Consumers' Accounts", December 23rd 2014, link.
[23] AUTORITÉ DE LA CONCURRENCE & BUNDESKARTELLAMT, "Competition law and data", 10th May 2016, 24, link.

29. Other competition authorities recognize that privacy may be a non-price element of competition. For example, the Canadian Competition Bureau considers privacy to be a 'product quality' which can be a non-price dimension of competition:

> "*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*".[24]

30. Additionally, Terrell McSweeny, a former commissioner for United States Federal Trade Commissioner, acknowledges that "*consumer privacy can be a non-price dimension of competition."*[25]

31. There have been a number of recent decisions[26] to suggest that there is an interest in examining issues related to privacy through a competition lens, but at the same time there is sensitivity that the aims of competition policy objectives are distinct from that of data protection authorities. For example, the European Court of Justice has showed some refrain to integrate data protection law considerations in competition law assessments when stating: "*any possible issue relating to the sensitivity of personal data are not a matter of competitions law and must be resolved on the basis of the relevant provisions governing data protection.*"[27]

32. While certain remedies might be effective toward addressing harms to competition, they may at the same time raise or create privacy issues and collaboration between authorities is needed to alleviate this tension. This is illustrated by the decision of the French competition authority imposing interim measures on GDF Suez ordering it to give other market players access to customer information such as name, addresses, telephone numbers and consumption profiles.[28] After consultation with the French data protection authority, each one of the affected consumers was offered the possibility to opt-out from this sharing mechanism. In the absence of opposition within 30 days, the consumers' data would become automatically available to other potential suppliers.

33. Privacy legislation could also hypothetically raise competition considerations. For example, a data protection requirement for consent for certain uses of information could theoretically provide a competitive advantage to firms that already have a relationship with a consumer, and can more easily communicate to achieve that consent (effectively raising switching costs and dampening competition).

---

[24] COMPETITION BUREAU CANADA, "Big data and innovation: key themes for competition policy in Canada", 19 February 2018, 8, link.
[25] T. MCSWEENY, "Competition Law: Keeping pace in a digital age", April 15th 2016, pg. 8, link.
[26] See for example the decisions mentioned in paragraphs 90-94 of this report.
[27] CJEU, *Asnef-Equifax*, C-238/05, para 63.
[28] AUTORITE DE LA CONCURRENCE, Décision n° 14-MC-02 du 9 septembre 2014, link; I. DE GRAEF, "Data as essential facility", *Phd-thesis at KU Leuven* 2016, 310-315, link.

34. As illustrated by the examples outlined above, it is clear that the intersection of privacy, consumer protection, and competition, is no longer a prospective matter, but one that is currently upon us. This report will now turn to a consideration of collaboration approaches, strategies and other tools that would allow regulators in all realms to better identify, understand and confront the challenges in protecting individuals' rights across all three regulatory realms.

# CHAPTER 2

## Identifying and fostering (inter)national collaboration initiatives

35. This chapter focuses on initiatives and frameworks on both national and international levels, which can facilitate collaboration between privacy, consumer protection and other regulatory authorities. The pivotal role of personal data in the digital economy has created a challenge in oversight and protection for all of these authorities. Sound co-ordination in case handling and cross-sectoral dialogue among them have an important role to play in identifying best practices to ensure that consumers' privacy rights are respected while simultaneously preserving the innovative potential of the digital economy.

### National collaboration initiatives

36. According to recent statistics published in the OECD paper on consumer protection enforcement in a global digital marketplace, 87% of the OECD members have legal frameworks or some kind of other arrangements to co-operate with other domestic authorities in the enforcement of consumer protection laws.[29] Notably, some of these inter-agency co-operation agreements relate to data protection issues.

37. Agencies have a keen interest in identifying concrete examples of domestic inter-agency collaboration and sketching an overview of some key factors and issues to take into account when doing so. For example, on specific cases, privacy will be looked at as an element of quality, or data as competitive advantage in competition law matters. In such cases the data protection authorities within the same jurisdiction may wish to provide input or comment on the way in which those privacy or data protection issues are considered. There are overlaps in respect of deception (relating to consent or identifying the ways in which information will be used) that may warrant *ad hoc* intervention when such cases present themselves. Scams and fraud are other areas where collaboration may be useful—privacy issues may uncover frauds and scams, and *vice versa*—so mechanisms to co-ordinate with those authorities responsible (whether consumer protection or otherwise) may be beneficial in the pursuit of protecting the citizenry.

38. The sections below highlight two examples of inter-agency collaboration that may be of interest to authorities looking to set up co-operation mechanisms on a domestic level.

[29] OECD, "Consumer protection enforcement in a global digital marketplace", *OECD Digital Economy Papers* 2018, no. 266, link.

## The smart watches case - co-operation between data and consumer protection authorities in Norway

39. The Norwegian Data Protection Authority (Datatilsynet), the Norwegian Consumer Protection Authority and the Norwegian Consumer Council have seen the importance of working together to strengthen consumer rights in the digital economy. The authorities have developed close co-operation on policy and enforcement issues. The data and consumer protection authorities have drawn 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.

40. For the past years, the Consumer Council has analyzed terms and conditions in so-called "smart products" such as fitness trackers, toys, health apps and GPS watches. Their analysis shows that there are major challenges related to data security when it comes to “Internet of things” devices. In 2017, the Consumer Council conducted an investigation into the security of various types of GPS watches marketed to children. The investigation showed that it was possible for unauthorized persons to extract information from the watch, as well as to read and change its location data. It was also possible to link the watch to a new account without the owner’s knowledge. These shortcomings constituted several breaches of European data and consumer protection laws.

41. In the wake of their findings, the Consumer Council submitted complaints regarding three GPS watches to the data protection authority and the consumer protection authority. These two authorities addressed the cases in co-ordination. Case handlers from both authorities worked together in order to make preliminary assessments of the cases and to outline the main concerns pursuant to the authorities’ respective legal frameworks.

42. When assessing the privacy policies, and terms and conditions, respectively, the authorities compared requirements in plain and intelligible language pursuant to data and consumer protection legislation. This ensured that the two authorities applied similar criteria to the documents and harmonized their approach.

43. As for the security issues, the authorities agreed that a reasonable course of action was for the data protection authority to first assess the cases from a data protection point of view and take enforcement actions accordingly. The outcome of the assessment and enforcement efforts would then have bearing on how the case would be assessed pursuant to consumer protection legislation.

44. At the outset, the authorities identified three outcomes. First, if data controllers would not comply with data protection legislation, it would be difficult for them to

continue to market and sell the devices pursuant to consumer protection law. Second, if data protection legislation would not be able to address all concerns because of jurisdictional challenges, consumer protection law could be used to impose duties on controllers to inform consumers about (surprising) data processing activities and risks to data protection. Third, if controllers would fully comply with data protection legislation, consumer protection law was unlikely to add additional information requirements, as long as the processing was not surprising to consumers or of a different nature than the consumers would reasonably expect based on the products' characteristics and marketing.

45. The data protection authority decided, after assessing the cases, to order the three controllers to cease processing of all personal data relating to the GPS watches due to poor security of processing. As a result of this order, one of the three data controllers decided to terminate its services. In the remaining two cases, the consumer protection authority is now making their own assessments, however, these assessments do not substantially concern the intersection of consumer and data protection.

## Dutch collaboration agreement between the data protection and consumer protection authority

46. The Dutch data protection authority (Autoriteit Persoonsgegevens) and the Dutch consumer protection and competition authority (Autoriteit Consument en Markt) concluded a collaboration agreement in 2016 to clarify the procedures to follow in case their respective competencies overlap or intersect.[30] The collaboration agreement states explicitly that concluding such an agreement has both the benefit of avoiding *ad hoc* agreements for each separate case and also establishing a co-operation framework that is transparent to all stakeholders.

47. The collaboration agreement formalizes some co-ordination mechanisms such as a yearly meeting on their ongoing co-operation, the designation of a distinct contact person within each authority and an evaluation of its functioning every three years. In addition, the agreement provides for information exchange and co-operation in case of concurrent competencies. The provisions on information exchange stipulate that both authorities can, and if asked are obliged to, share information that is necessary to carry out their respective legal missions. Also, the authorities inform each other when they are confronted with a violation that is exclusively situated within the competencies of the other authority. In case of concurrent competencies, both authorities need to consult in order to determine who will handle various aspects of the case. The authorities can also choose to establish a joint team to

[30] ACM & AP, "Samenwerkingsprotocol tussen Autoriteit Consument en Market en Autoriteit Persoonsgegevens", *Staatscourant* 3 November 2016, link.

handle the case. The collaboration agreement also contains provisions on the competence to enforce specific provisions, for example, on cookies and direct marketing.

48. Both authorities have established a long-term working relationship based on the collaboration agreement and worked on several privacy issues for consumers in the past. For example issues like lead generation, deep packet inspection or the collection of sensitive personal of consumers data during elections[31].

## International collaboration initiatives

49. Parallel to national inter-agency collaboration, the digital economy also requires a well-functioning framework for international co-operation and enforcement. The sections below summarize certain international initiatives aiming to improve international enforcement co-operation and promote better dialogue among different authorities.

### The Global Privacy Enforcement Network's Network of Networks Initiative

50. The Global Privacy Enforcement Network's ("GPEN") Network of Networks ("NoN") initiative aims improve international enforcement co-operation by promoting better dialogue among relevant networks of privacy enforcement authorities and establishing dialogue with enforcement authorities from other sectors. This second part is particularly relevant to the work of the Working Group. By engaging in exchanges with consumer agency participants of the GPEN NoN, privacy authorities may find better opportunities for international co-operation.

51. The Unsolicited Communications Enforcement Network ("UCENET", formerly the London Action Plan) and the International Consumer Protection and Enforcement Network ("ICPEN") both participate in the GPEN NoN initiative. UCENET was founded in 2004 with the purpose of promoting international spam enforcement co-operation. Since inception, UCENET has expanded its mandate to include additional online and mobile threats, including malware, SMS spam and "do not call". UCENET membership includes representatives from the government regulatory and enforcement community and interested industry members.

52. ICPEN works to promote and facilitate consumer protection enforcement, including through information sharing on market developments and regulatory best practices, as well as co-ordination and co-operation to tackle market problems. In recent years this also includes a growing emphasis on inter-agency co-operation on consumer protection enforcement projects. ICPEN also runs econsumer.gov, a website where

[31] ACM, "ACM and the Dutch DPA take action against Stemwijzer.nl", 8 February 2017, link.

consumers worldwide can report international scams. Consumer agencies from 36 countries participate in econsumer.gov. The project has two main components: a multi-lingual public website that allows consumers to make cross-border fraud complaints; and a secure econsumer.gov website that allows law enforcement around the world to share and access consumer complaint data and other investigative information from other jurisdictions.

53. The NoN initiative primarily serves to allow GPEN to learn how other sectors co-operate, in order to improve GPEN's own co-operation models. A secondary benefit is the possibility for exchanges on common problems, so as to develop inter-network co-operation. GPEN members have been invited to attend the ICPEN conference as an observer organisation. This relationship allows GPEN to further its understanding of the importance, and increasing prevalence, of matters where privacy and consumer protection enforcement intersect. Specifically, the GPEN's attendance at ICPEN as an observer allows each respective network to benefit from each other's relevant knowledge and enforcement experience. For example, by sharing best practices, confronting matters of mutual interest and to develop bilateral and multilateral relationships that facilitate further cross-sectorial co-operation.[32]

## OECD Recommendation on Cross-border Co-operation in the Enforcement of Laws Protecting Privacy

54. In 2007, the OECD issued a recommendation[33] containing several features which could facilitate co-operation between privacy and consumer protection authorities. Focusing on "Laws Protecting Privacy" (meaning "national laws or regulations, the enforcement of which has the effect of protecting personal data consistent with the OECD Privacy Guidelines"), it recommends that countries "improve their domestic frameworks for privacy law enforcement to better enable their authorities to co-operate with foreign authorities." Specifically, the OECD recommends that: data protection or privacy authorities be given mechanisms to share relevant information with foreign authorities relating to possible violations of laws protecting privacy; and data protection or privacy authorities be able to provide assistance to foreign authorities (relating to possible violations of their law protecting privacy), with

[32] In a 2018 open letter to digital economy businesses, members of ICPEN identified concerns regarding practices that "could harm consumers and may not comply with national consumer laws." The letter includes in its assessment of these harms, matters concerning privacy, such as, avoidance of lengthy terms and conditions that discourage individuals from engaging important information regarding privacy and privacy rights. ICPEN, "Joint open letter to businesses in the digital economy on the importance of standard terms and conditions for consumers", 29 June 2018, link.

[33] OECD, "Recommendation on cross-border co-operation in the enforcement of laws protecting privacy", 2007, link.

regard to obtaining information from persons; obtaining documents or records; or locating or identifying organisations or persons involved.

55. Another general recommendation is for appropriate steps to be taken to "engage relevant stakeholders in discussion and activities aimed at furthering co-operation in the enforcement of laws protecting privacy." While this could include consumer authorities, the specific examples later given include: criminal authorities; privacy officers and private sector oversight groups; and civil society and business groups. The spirit that animates the general recommendation could certainly extend to consumer authorities. However, the specific examples provide indirect support for the view that the whole recommendation, covering laws with "the effect of protecting personal data" include consumer law.

## GPEN practitioner's event

In 2018, GPEN held its second "practitioner's event". The event provided an opportunity for GPEN members to engage in discussions at a staff or "practitioner" level. The focus was on the practical aspects of investigation, enforcement, and post-enforcement stages of a case. The aim of the event was to: share practical experiences, skills and strategies relevant to enforcement in the context of online practices within and outside domestic borders; and develop operational-level relationships that will create the foundation for future collaboration.

56. This year's event was open to the GPEN NoN participants, including UCENET and ICPEN. Attendance and active participation by consumer authorities promotes further co-operation between privacy and consumer authorities and facilitates skill and experiential transfer across regulatory spheres.

## Digital Clearinghouse

57. The Digital Clearinghouse aims to convene regulators of different areas of law, such as data protection, consumer protection and competition enforcement, with a view to addressing common concerns and fostering a frank dialogue on issues at the intersection of laws. The Digital Clearinghouse works on the idea that, as the digital economy puts the protection of rights and interests of the individual under unprecedented strains, a steadily coherent and "no-silos" response is needed from all regulators responsible for the digital ecosystem. The network was launched upon

the initiative of the EDPS.[34] It has been endorsed by the European Parliament[35] and supported by the 39th ICDPPC.[36]

58. Regulators met twice in 2017, and a third meeting occurred in June 2018. The intersection of laws and common concerns were explored including: information disparities between individuals and service providers; attention markets and opacity of algorithms collecting and using personal data; privacy by design and product safety failures in connected things; micro-targeting and voter manipulation; collusive and personalised pricing; terms and conditions of free online services and fairness of privacy policies; and the relevance of personal data for competition and consumer assessment.

59. Co-operation mechanisms across boundaries were also discussed. For example, data protection authorities' support to competition regulators in digital mergers, and joint endeavours between data and consumer protection agencies were topics covered.

## Collaboration mechanisms

60. The remainder of this chapter provides an overview of collaboration mechanisms, both formal and informal, that might inspire various authorities active in enforcement in the digital ecosystem toward further co-operation.

### Secondments / Staff Exchanges / Fellowships

61. Staff exchanges, fellowships or secondments can directly foster collaboration and information exchanges between agencies. A secondee can assist the host agency with understanding matters related to the home agency. Conversely, the secondee, upon return, brings to the home agency insights into how the host agency operates. Finally, secondments build a staff-level familiarity, relationships, and trust that is often crucial to effective co-operation. Secondees can become key points of contact for initiating future collaboration efforts. Several initiatives exist to promote secondments:

- APPA Secondment Framework.[37] The Asia-Pacific Privacy Authorities ("APPA") forum issued a Secondment Framework in December 2014. The

[34] EDPS, "Opinion 8/2016 on Coherent enforcement of fundamental rights in the age of Big Data", 23 September 2016, link.
[35] EUROPEAN PARLIAMENT, "Resolution on Fundamental rights implication of Big Data", 20 February 2017, link.
[36] ICDPPC, "Resolution on Collaboration between Data Protection Authorities and Consumer Protection Authorities for Better Protection of Citizens and Consumers in the Digital Economy", 26-27th September 2017, Hong Kong, link.
[37] http://www.appaforum.org/resources/secondments/.

framework provides advice on setting up a successful secondment, including suggestions of how they should be organized; a chronological checklist; and other materials aimed at the secondee, the home manager, and the host managers.

- GPEN Opportunities Panel. The GPEN website forum hosts an opportunities panel where agencies can post secondment or job opportunities.

- EDPB Secondment. Seconded national experts ("SNEs") are sometimes seconded to the Secretariat of the European Data Protection Board ("EDPB") for a fixed-term from the staff of national public-sector bodies in the EU member states. SNEs gain valuable experience at EU level and allow the EDPB to benefit from their professional skills and experience. When there is an opening for an SNE, the EDPB contacts the national data protection authorities with a call for applications. Applications are done through their employer, who continues to pay their salary during the secondment.[38]

62. The Working Group notes the potential in secondments and assignments between data protection, competition and consumer authorities within the same jurisdiction can be a useful mechanism for expanding an agency's perspective. In addition, inter-agency exchanges can help to build expertise across multi-disciplinary enforcement areas, as well as develop informal contact networks at the staff level to ensure that collaboration, when pursued, is effective.

## Referrals

63. Referrals between jurisdictions can assist an agency in achieving its mission, leveraging work already done by another agency. This can happen in various circumstances, such as when it has already acted to the extent of its powers or has jurisdictional or other hurdles to continuing an enforcement matter. Realistically, these boundaries are often not fixed, but a matter of resource hurdles. A long-shot jurisdictional argument could be made and won, but would take on significantly more resources, reducing resources available for other matters. In such situations, referrals may be an appropriate way to leverage work that has already been done to further advance the matter consistent with the agency's mission.

64. Typically, the evidence or other information gathered on a matter is organized, shared with, and explained to another agency. Staff from the referring agency remain available to answer questions or provide authentication as needed. The form of referral relationships can vary. The receiving agency may or may not be

[38] https://edpb.europa.eu/about-edpb/career-opportunities_en

obligated to act on the matter. Likewise, the referring agency may or may not be entitled to a response or update from the receiving agency.

65. Examples of referral programs include:

- FTC Criminal Liaison Unit ("CLU").[39] The US FTC has a dedicated unit for liaising with and referring matters to criminal prosecutors. A similar effort could be carried out at a privacy agency to refer matters to consumer agencies. US FTC fraud cases can develop evidence that supports criminal prosecutions, such as victim statements, undercover purchases, business records, and inside testimony. The CLU team helps prosecutors understand the evidence, including how a complex fraud operates, and often can also point to a successful civil case already brought by the FTC. As a result, prosecutors are more likely to bring criminal charges since they are handed a more mature case file.

- GPEN Alert. The GPEN Alert mechanism provides a short-hand referral system. Participating authorities can, confidentially, signal their interest in a given matter or investigation, seeking co-operation opportunities.

## Regional collaboration mechanisms (an EU example)

66. In addition to international collaboration mechanisms, there are institutionalized regional co-operation frameworks. The two mechanisms outlined below entail co-operation within the EU in the fields of consumer protection and data protection. The mechanisms they introduce can also spark inspiration for collaboration across the lines of consumer protection, privacy and competition law both on a national and international level.

- The EU's Consumer Protection Co-operation Regulation Network ("CPC network"). This network enables consumer authorities to take part in joint enforcement actions whenever breaches of consumer protection rules occur in different jurisdictions across the European Economic Area.[40] Within the CPC network any authority in a country where consumers' rights are being violated can ask its counterpart in the country where the business is based to take action. The Consumer Protection Co-operation Regulation sets a list of minimum powers which each authority must have to ensure smooth co-operation. These include power to obtain the information and evidence needed to tackle infringements within the EU; conduct on-site inspections; require cessation or prohibition of infringements committed within the EU;

[39] http://www.appaforum.org/resources/secondments/

[40] EUROPEAN COMMISSION, "Single Market Scoreboard – Consumer Protection Cooperation Network", Reporting period January – December 2017, link.

and obtain undertakings and payments into the public purse from businesses. The CPC network provides a platform where consumer protection authorities can alert each other to malpractices that could spread to other countries. Furthermore, it allows them to co-ordinate their approaches to applying consumer protection law so as to tackle widespread infringements.

Recently a new CPC-regulation has been adopted: CPC-regulation (EU) 2017/2394 . The new regulation will be applicable as of 17 January 2020 and intends to improve the current CPC framework by reinforcing the mutual assistance mechanism (by imposing tighter deadlines), extending the minimum powers accorded to national consumer protection authorities and establishing a better coordination mechanism for widespread infringements that are likely to harm the collective interests of consumers residing in multiple Member States.

- The EU General Data Protection Regulation ("GDPR") introduced a similar obligation imposed on data protection authorities to provide each other with relevant information and mutual assistance in order to implement and apply the GDPR in a consistent manner. Mutual assistance covers information requests and supervisory measures, such as requests to carry out prior authorisations and consultations, inspections and investigations. Each data protection authority must reply to a request from another supervisory authority without undue delay and no later than one month after receiving the request. Such measures may include, in particular, the transmission of relevant information on the conduct of an investigation. Requests for assistance must contain all the necessary information, including the purpose of, and reasons for, the request. Information exchanged shall be used only for the purpose for which it was requested.

67. The GDPR also opens up a formal framework for joint operations including investigations and enforcement measures in which members or staff of the supervisory authorities of multiple member states are involved. If the controller or processor has establishments in several member states or where a significant number of data subjects in more than one member state are likely to be substantially affected by processing operations, a supervisory authority of each of those member states has the right to participate in such joint operations.

68. Despite these examples of both national and international collaboration initiatives the Working Group notes that there remains a considerable potential to foster informal collaboration and promote sound examples of well-established and functioning formal co-operation frameworks. The Working Group suggested consideration be given to organizing workshops, webinars, and teleseminars, in the future dealing with inter-agency collaboration questions and creating a more established presence of the Working Group in international fora such as ICPEN, GPEN, and the Digital Clearinghouse. A particular focus should be put on formal

and informal frameworks that allow for issuing alerts possibly relevant to other authorities; inter-agency sharing of (confidential) information; possibilities to conduct joint enforcement actions; and exchange best practices and lessons learned from specific cases.

# CHAPTER 3

## Substantive Challenges and Overlaps

69. As highlighted throughout this report, data protection, consumer protection and competition law offer various legal instruments to deal with commercial practices that exploit personal data in ways that are inappropriate. In some cases, they offer remedies that coincide. In other cases, the differences in the underlying objectives pursued by these distinct areas of law, lead to tension as the solutions offered by one of them might be in conflict with the others.

70. This chapter discusses selected key substantive principles that are common to privacy, data protection, and consumer protection and to a certain extent competition law, including fairness and consent.

### Fairness

71. Fairness is a principle common to privacy, data protection and consumer protection. Although the concept of fairness is interpreted differently across these areas of law, the realities of today's digital economy may lead to more converging interpretations.

72. In EU data protection legislation, for example, the notion of fairness is embedded in article 5.1.a) of the GDPR which reads as follows:

*"Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency')"*

73. Generally speaking, fairness is intimately linked to the level of information given to the data subject insofar as a data subject who has been given insufficient amounts of information is not in a position to make an autonomous decision over their personal data.[41] Recital 39 of the GDPR confirms this approach "*any processing of personal data should be lawful and fair. It should be transparent to natural persons that personal data concerning them are collected, used, consulted or otherwise processed and to what extent the personal data are or will be processed.*"[42]

[41] W. MAXWELL, "The Notion of 'Fair Processing' in Data Privacy" in *Quelle protection des données personnelles en Europe?*, CÉLINE CASTETS-RENARD (ed.), University of Toulouse, 2015, link.
[42] See also recital 60 GDPR: "The principles of fair and transparent processing require that the data subject be informed of the existence of the processing operation and its purposes."

74. Under EU data protection legislation it is clear that a lack of information results in unfair processing, however, it has been less clear what other practices fall within the ambit of the fairness threshold. To that end, a recent case from the Belgian Court of First Instance appears to open up the fairness criterion[43].

75. The case is based on an investigation by the Belgian data protection authority into Facebook which found that Facebook collects information concerning every Internet user when they browse the Internet, not only on the Facebook platform but also from more than 10,000 different websites. To accomplish this, Facebook uses various technologies, such as "cookies", "social plug-ins" (for example, the "like" or "share" buttons), and "pixels" (which are invisible images used to track browsing behaviour), such that even if an individual has never visited the Facebook domain, their browsing behaviour is still tracked discreetly in the background by Facebook.

76. In its decision, the Belgian Court of First Instance stated:

> "*Honest (sic) processing requires the data to be transparently obtained, not kept for longer than is necessary and that their later processing should not be contrary to the reasonable expectations of the party involved. […] the lack of information not only hinders legally valid consent, but also the honest processing of personal data.*"[44] (emphasis added)

77. The above quote demonstrates the Court's link between informed consent and the fair or honest processing of data, noting that a lack of information hinders obtaining legally valid consent *and* the honest processing of personal data. Substantively speaking, this judgment raises the idea of fairness in data protection as well as consumer protection by introducing the reasonable expectations of the consumer as one of the criteria to assess the fairness of a processing operation.

78. Similarly, a recent undertaking proposed to WhatsApp by the United Kingdom's Information Commissioner's Office ("UK ICO") confirms that fairness remains linked to the requirement to provide sufficient information, reading in part: "*the purported consent was not fairly obtained. In relation to existing users, the process did not inform users with sufficient clarity that their personal data was to be shared with Facebook for any of the purposes. The first layer of the notice did not mention Facebook at all […]*"[45]

[43]The Belgian court of first instance rendered this part of its judgment on article 4, section 1 of the Belgian Privacy Act of 8 December 1992 which transposed article 6.1.a) of the European Data Protection Directive 95/46/EC and was repealed and replaced by the GDPR on 25 May 2018. Although the wordings of the new article 5.1.a) of the GDPR are slightly different, the essence of this provision remained unaltered.

[44] BRUSSELS COURT OF FIRST INSTANCE, judgment of 16 February 2018, 66, link.

[45] INFORMATION COMMISSIONER'S OFFICE, Letter to WhatsApp concerning the sharing personal data between WhatsApp Inc. ("WhatsApp") and the Facebook family companies, 16 February 2018, 6, link.

79. From a consumer protection standpoint, fairness is a core objective. In the EU, for example, the most relevant instrument dealing with fairness is the Unfair Commercial Practices Directive ("UCPD").[46] Specifically, Article 5(4) of the UCPD specifies two particular categories of unfair practices: misleading practices; and aggressive commercial practices[47]. The UCPD defines these two categories as follows:

> "***Art. 6 – Misleading actions***
>
> *A commercial practice shall be regarded as misleading if it contains false information and is therefore untruthful or in any way, including overall presentation, deceives or is likely to deceive the average consumer, even if the information is factually correct, in relation to one or more of the following elements, and in either case causes or is likely to cause him to take a transactional decision that he would not have taken otherwise: […]*
>
> ***Art. 8 – Aggressive commercial practices***
>
> *A commercial practice shall be regarded as aggressive if, in its factual context, taking account of all its features and circumstances, by harassment, coercion, including the use of physical force, or undue influence, it significantly impairs or is likely to significantly impair the average consumer's freedom of choice or conduct with regard to the product and thereby causes him or is likely to cause him to take a transactional decision that he would not have taken otherwise.*"

80. Whether a privacy-related issue will necessarily be considered a violation of consumer protection law is addressed by the European Commission's guidance on the UCPD:

> "*A trader's violation of the Data Protection Directive or of the ePrivacy Directive will not, in itself, always mean that the practice is also in breach of the UCPD. However, such data protection violations should be considered when assessing the overall unfairness of commercial practices under the UCPD, particularly in the situation where the trader processes consumer data in violation of data protection requirements, i.e. for direct marketing purposes or any other commercial purposes like profiling, personal pricing or big data applications.*"[48]

---

[46] Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 *concerning unfair business-to-consumer commercial practices in the internal market and amending Council Directive 84/450/EEC, Directives 97/7/EC, 98/27/EC and 2002/65/EC of the European Parliament and of the Council and Regulation (EC) No 2006/2004 of the European Parliament and of the Council* ('Unfair Commercial Practices Directive').

[47] The general clause of article 5(2) of the UCPD and the two categories of unfair commercial practices are complemented by a blacklist annexed to the UCPD. The general clause of article 5(2) of the UCPD can be used as "safety net" for practices that are not captured by the blacklist or the more specific clauses on aggressive and misleading practices.

[48] EUROPEAN COMMISSION, "Guidance on the implementation/application of directive 2005/29/EC on unfair commercial practices", SWD(2016) 163final, 25 May 2016, link.

81. Therefore, a lack of transparency on personal data processing should be considered when assessing the fairness of a business practice. Several recent cases illustrate the overlap between the UCPD and data protection principles.

82. For example, on January 16th 2018, the Berlin Court of Appeal declared several provisions of Facebooks privacy policy to be illegal.[49] The Court found Facebook in breach of German data protection law and consumer law with respect to Facebook's default privacy settings and certain Facebook terms and conditions. The Court found that users did not consent to certain pre-checked settings such as, sharing location data with other users while chatting and having a user's timeline being searchable via search engines. Furthermore, the Court found that Facebook's terms and conditions were invalid since they were framed too broadly to include "*pre-formulated declarations of consent, which allowed Facebook to use the name and profile picture of users "for commercial, sponsored or related content.*"[50]

83. On the one hand the Court used data protection legislation to address the default settings of the Facebook app, reasoning that the app did not collect informed consent. On the other hand, the Court annulled several clauses from Facebook's terms and conditions on the basis they are contrary to the UCPD. While the Court used consumer protection legislation to strike the offending clauses down, the substantive analysis of 'unfairness' relied heavily on data protection law (in particular, the provisions on informed consent.) This judgment represents an excellent illustration of the interplay between data protection and consumer protection legislation.

84. More recently, in April 2018, the Italian antitrust and consumer protection authority ("AGCM") launched an investigation into Facebook over alleged unfair commercial practices.[51] This investigation is evaluating whether Facebook properly informed users adequately and immediately during account activation of the collection and use of user data and whether this behaviour is an unfair commercial practice in violation of the Italian Consumer Code (which transposes the UCPD in Italian national law). This case has the potential to illustrate the interaction between privacy, data protection and consumer protection through the application of consumer protection frameworks against practices that typically fall within the ambit of data protection legislation.

[49] Cfr. Press release of the claimant; BERLIN REGIONAL COURT, judgment of 24 January 2018, link.

[50] Ibid.

[51] L'AUTORITÀ GARANTE DELLA CONCORRENZA E DEL MERCATO, "Misleading information for collection and use of data, investigation launched against Facebook", 6 April 2018, link press release.

85. Whereas enforcement of privacy issues through consumer protection legislation is still in its relative infancy in the EU, the US FTC is very familiar with this approach which is embedded in its dual mandate.[52] For instance, section 5 of the US FTC Act prohibits "*unfair or deceptive acts or practices in or affecting commerce*". Unfairness is further defined in the legislation:

> "*The Commission shall have no authority under this section or section 57a of this title to declare unlawful an act or practice on the grounds that such act or practice is unfair unless the act or practice causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition.*"[53]

86. In order for a practice to be considered unfair the US FTC needs to establish that the practice causes a substantial injury that consumers cannot reasonably avoid, and this injury is not offset by countervailing benefits. Unlike the UCPD, where misleading practices are a subcategory of unfair practices, the US FTC has a separate analysis to assess whether a practice is deceptive. For a practice to be deceptive, there must be a representation, omission or practice that is likely to mislead the consumer, acting reasonably under the circumstances; and the representation, omission, or practice must be a "material" one.[54]

87. The Working Group notes that in certain cases, a tendency exists to resolve privacy issues by the means of consumer protection legislation. Nevertheless, even in cases of enforcement through consumer protection legislation, data protection and privacy remain key criteria in the substantive assessment of the fairness and illegality of terms and conditions and other commercial practices, resulting in an intimate overlap of both areas of law.

## Consent as a common issue

88. As described above, the practices of a business or data controller can include complex and misleading terms and conditions to an extent that consumers' and data subject's consent is unreliable and their autonomy of choice is reduced when accepting privacy terms. The ability to make effective choices is key in consumer protection, data protection and competition law. For instance, consent is prevalent in decisions taken by the Italian antitrust and consumer protection authority and the

[52] W. MAXWELL, "The Notion of 'Fair Processing' in Data Privacy" in *Quelle protection des données personnelles en Europe?*, CÉLINE CASTETS-RENARD (ed.), University of Toulouse, 2015, link.
[53] 15 U.S.C. §45(n)
[54] FTC, "Policy Statement on Deception", 1983, link.

preliminary assessment of the German competition authority in its proceedings against Facebook.

89. On May 11th 2017, the AGCM adopted two decisions stemming from two investigations against WhatsApp concerning the requirement that users accept its terms and conditions and the quasi-unilateral change of its terms and conditions.[55] The first investigation showed that the way in which WhatsApp sought to extract user consent for transferring consumer data to Facebook constituted an unfair and aggressive commercial practice according to the Italian Consumer Code (which implements the provisions of the UCPD).[56] The authority also determined that making the use of WhatsApp conditional on the full agreement to revised terms and conditions (including sharing data with Facebook) led users to believe they would otherwise lose access to WhatsApp. This represented an aggressive commercial practice. Since the possibility of not consenting to data sharing was not presented on the main page, the commercial practice limited the user's freedom of choice, leading them to take a decision that they may not have otherwise taken.[57]

90. Further, the practices of WhatsApp were found to violate article 8 of the UCPD, which prohibits aggressive practices, including undue influence, as an unfair commercial practice. Specifically, WhatsApp was found to be exerting "undue influence" over its users, leading them to grant broader consents than were necessary to continue using the service. Moreover, the ACGM found that the undue influence finding was aggravated given the market dominance of both WhatsApp and Facebook. The practice was deemed to be in breach of the professional diligence that a user would reasonably expect from a leading service provider in the market for consumer communication services.[58]

91. As described under "Fairness" above, the ACGM's recent (2018) investigations against Facebook[59] are examining the use of pre-selection to enable exchanges of personal data to and from third parties every time the user accesses or uses third-party websites and apps, only providing an opt-out option. It is alleged that Facebook may be exercising undue influence on registered users, who, in exchange for using Facebook, consent to the collection and use of all the information

[55] L'AUTORITÀ GARANTE DELLA CONCORRENZA E DEL MERCATO, Decision 11 May 2017, link press release, link PS10601, link CV154; N. ZINGALES, "Between a rock and two hard places: WhatsApp at the crossroad of competition, data protection and consumer law", *Computer law & security review* 2017, Vol(3), 553-558.

[56] The authority remarked that the behaviour was not, as such, forbidden by the Italian data protection law, but it was found to be in breach of Italian consumer law. AUTORITÀ GARANTE DELLA CONCORRENZA E DEL MERCATO, Decision 11 May 2017, p. 13, link.

[57] The user would have realised having an alternative only on a subsequent step, after agreeing to the revised terms and accessing the privacy policy. Moreover, that not-self-evident option was set as an opt-out option. In sum users were induced to provide a wider consent than needed to keep on using the app.

[58] *Ibid.*

[59] L'AUTORITÀ GARANTE DELLA CONCORRENZA E DEL MERCATO, "Misleading information for collection and use of data, investigation launched against Facebook", 6 April 2018, link press release.

concerning them, for example: information from their personal Facebook profiles, those deriving from the use of Facebook and from their own experiences on third-party sites and apps.

92. A similar line of reasoning can be found in the preliminary assessment of the German competition law authority (Bundeskartellamt) in its investigation into Facebook's terms and conditions. According to the Bundeskartellamt's preliminary assessment, Facebook is imposing unfair terms and conditions on its users, under German law, by making them choose between accepting 'the whole Facebook package' and 'none of it'. After having stated the reasons why Facebook is considered to occupy a dominant position, the Bundeskartellamt frames the abuse in the following terms:

> "*If a dominant company makes the use of its service conditional upon the user granting the company extensive permission to use his or her personal data, this can be taken up by the competition authority as a case of "exploitative business terms". […] such exploitation can take the form of excessive prices (price abuse) or unfair business terms (exploitative business terms)*".

The Bundeskartellamt continues:

> "*[…] civil law principles can also be applied to determine whether business terms are exploitative. On principle, any legal principle that aims to protect a contract party in an imbalanced position can be applied for this purpose. Following the [German] Federal Court of Justice's approach, the Bundeskartellamt also applies data protection principles in its assessment of Facebook's terms and conditions*. […] *Data protection legislation seeks to ensure that users can decide freely and without coercion on how their personal data are used*."

93. It should be noted that the reasoning of the Bundeskartellamt is rooted in their domestic law and jurisprudence, which allows the agency to use the violation of data protection provisions as proof of abuse. Another provision within domestic German competition law considers access to personal data a criterion for market power. Nevertheless, this case does raise the question whether and under which conditions a violation of data protection legislation can lead to competition law violations[60].

94. These are just some of the recent examples of the overlap in application of data, privacy, and consumer protection laws. As the digital economy grows so too will

[60] See in this respect: G. COLANGELO & M. MARIATERESA, "Data accumulation and the privacy-antitrust interface: Insights from the Facebook case for the EU and the US", *TTLF Working Papers* 2018, n° 31.

the frequency of such incidents posing cross-jurisdictional challenges, and the need for continued co-operation across regulatory disciplines.

# CHAPTER 4

## Further action of the Working Group

95. In the light of the considerations above there is a clear need to continue exploring this important intersection. To this end, the Working Group has submitted a resolution for the ICDPPC's consideration and adoption.

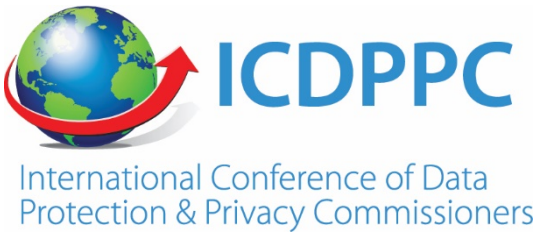
96. The draft resolution tasks the Working Group with:

i. reaching out to more authorities competent for consumer, privacy, data protection and competition enforcement in an effort to analyze and map interesting enforcement cases and jurisprudence affecting the privacy of digital consumers with a view to providing additional insight into decision-making and identifying collaboration opportunities as they arise;

ii. creating an established presence of the Working Group in international fora such as ICPEN, GPEN, the Digital Clearinghouse and the Consumer Protection Co-operation Network with a view to supporting the influence of the Working Group at these networks, to promote privacy considerations at consumer protection fora, and to facilitate ongoing inter-agency awareness and cooperation at an international level; and

iii. considering the development of a workshop or webinar series on inter-agency co-operation to identify frameworks and best practices on the conclusion of inter-agency agreements, information exchange and joint enforcement actions. For example, this may be accomplished by organizing a workshop and extending invitations to networks exploring the intersection (such as those stated in task 2) and by leveraging the work of other ICDPPC working groups (such as the Enforcement Working Group) with a view to identifying successful collaborative efforts, challenges and opportunities.

# Appendix B: DCCWG Resolution passed at 40th International Conference




# RESOLUTION ON COLLABORATION BETWEEN DATA PROTECTION AUTHORITIES AND CONSUMER PROTECTION AUTHORITIES FOR BETTER PROTECTION OF CITIZENS AND CONSUMERS IN THE DIGITAL ECONOMY

40th International Conference of Data Protection and Privacy Commissioners
Tuesday 23rd October 2018, Brussels

*AUTHOR:*

- Data Protection Authority, Belgium – on behalf of the Digital Citizen and Consumer Working Group.

*CO-SPONSORS:*

- Data Protection Commission, Ireland
- European Data Protection Supervisor
- Information Commissioner's Office, UK
- Datatilsynet (Data Inspectorate), Norway
- Office of the Privacy Commissioner of Canada
- Privacy Commissioner for Personal Data, Hong Kong

NOTING that:

a) Statutory protections for individuals, whether as citizens or consumers, are imbedded in consumer protection, privacy and data protection laws;

b) the Conference's strategic priority includes the strengthening of our connections and work with partners to achieve our mission of supporting authorities more effectively to include the protection of personal data in their mandates;

c) the Conference is committed to addressing the challenges related to privacy and data protection in the digital age;

d) individuals are increasingly concerned about their lack of control over, and information about how, their information is processed and protected in the online environment;

e) data protection authorities should cooperate with appropriate bodies that can achieve the goal of protecting the rights of the individual in relation to their personal data;

f) personal information is increasingly a core part of business models in the digital economy;

g) in its statement of the 27th of August 2018 the European Data Protection Board voiced the concern that "*increased market concentration in digital markets has the potential to threaten the level of data protection and freedom enjoyed by consumers of digital services" ;*

h) privacy and data protection are becoming important considerations informing consumer decisions in the digital economy; and

i) Accordingly, there is a growing intersection of consumer protection, data protection and privacy issues.

RECALLING that:

a) the 39th Conference resolved to identify the need for, and highlight ways to improve, collaboration between data protection and consumer protection authorities at both domestic and international levels with a view to fostering better protection for citizens and consumers in the digital economy;

b) the 39th Conference established the Digital Citizen and Consumer Working Group which was tasked to report back to the 40th Conference on the current legal and practical state of collaboration between data protection authorities and consumer protection authorities, and to submit a resolution proposing specific measures or further concrete work.

HAVING READ the report of the Digital Citizen and Consumer Working Group

THE 40th CONFERENCE resolves:

1. to continue efforts to bring about effective inter- and intra-jurisdictional cooperation between data protection and consumer protection authorities in specific cases or categories of cases to improve outcomes for individuals' rights;
2. to consider the interaction of privacy, data protection, regulation, and competition and their implications for consumers;
3. to continue to study the overlap of substantive legislation affecting the rights of digital consumers;
4. to renew and confirm the mandate of the Digital Citizen and Consumer Working Group which was originally conferred to it by the 39th Conference. In particular with a view to:
    a. increasing the presence of the Digital Citizen and Consumer Working Group at international fora that consider the intersection between consumer protection, privacy and data protection, including the International Consumer Protection and Enforcement Network (ICPEN), the Global Privacy Enforcement Network (GPEN), the Digital Clearinghouse (DCH) and Consumer Protection Cooperation Network (CPC);
    b. leveraging this presence to engage authorities competent for consumer, privacy, data protection as well as other relevant authorities such as competition and antitrust enforcement authorities in an effort to monitor and map relevant enforcement cases and jurisprudence affecting the privacy of digital consumers, for example, in order to better understand how to design multi-disciplinary approaches to statutory protections for individuals' data; and
    c. to report back to the 41st Conference on the elements listed above and if necessary submit a resolution proposing specific measures and/or further concrete work.

# Appendix C: DCCWG Workplan

# DIGITAL CITIZEN AND CONSUMER WORKING GROUP

# PROJECT MANAGEMENT PLAN

**Version 2.0**

**6/6/2019**

# TABLE OF CONTENTS

TABLE OF CONTENTS ..... 2
1. INTRODUCTION ..... 2
1.1 PURPOSE OF THE PROJECT MANAGEMENT PLAN ..... 2
2. EXECUTIVE SUMMARY OF THE DCCWG ..... 2
3. PROJECT GOALS, OBJECTIVES AND BUSINESS OUTCOMES ..... 3
3.1 LONG-TERM GOALS ..... 3
3.2 SHORT TERM GOALS ..... 3
3.2 STAKEHOLDERS ..... 4
3.3 OBJECTIVES ..... 4
4. MILESTONES ..... 5

## 1. INTRODUCTION

### 1.1 PURPOSE OF THE PROJECT MANAGEMENT PLAN

The *Digital Citizen and Consumer Working Group* ("DCCWG") Project Management Plan is intended to provide structure and vision to the DCCWG towards advancing the objectives of its resolutions.

## 2. EXECUTIVE SUMMARY OF THE DCCWG

The DCCWG was established in 2017 via a resolution passed at the International Conference of Data Protection and Privacy Commissioner's ("ICDPPC"). The DCCWG was tasked with exploring the intersection between privacy and consumer protection issues, laws and concepts.

Co-authored by the Belgian Data Protection Authority ("Belgian DPA"), the Office of the Privacy Commissioner of Canada ("OPC"), the United States Federal Trade Commission ("FTC"), and with contributions from the European Data Protection Supervisor ("EDPS"), the DCCWG completed a white paper exploring the intersection between privacy and consumer protection and citing examples of cooperation between privacy and consumer protection agencies. The DCCWG has also set a course for 2018-2019 through a further resolution to continue the analysis of the growing dynamic between competition and privacy.

Following inaugural leadership by the Belgian DPA, the OPC and the Office of the Australian Information Commissioner ("OAIC") will now act as co-chairs of the DCCWG during 2018-2019. The DCCWG work ahead includes engaging additional authorities across regulatory spheres to analyze and map enforcement cases and jurisprudence, increasing presence of the DCCWG and awareness of the privacy/consumer protection/competition intersection in international fora, and developing a workshop or webinar series to identify and develop best practices, foster information exchanges and potentially undertake cross-regulatory collaborative initiatives.

# 3. PROJECT GOALS, OBJECTIVES AND BUSINESS OUTCOMES

Our vision contemplates both long and short-term objectives.

## 3.1 LONG-TERM GOALS

Our long-term goal for the DCCWG is to advance the will and realize the mechanisms to collaborate and share information with enforcement partners across regulatory spheres, with a view to having holistic and efficient regulatory outcomes that provide a greater scope of coverage for consumers from privacy, consumer protection and competition risks.

## 3.2 SHORT TERM GOALS

Our short-term goals include continued expansion of regulatory awareness and collaboration on intersection issues, in particular for the areas beyond strictly consumer protection (for example, involving anti-trust and competition). To this end, we aim to: (i) advance the understanding and sensitize regulators across spheres about the intersection between privacy and consumer protection such that regulators in consumer protection can recognize a privacy issue and vice versa; (ii) identify in greater depth intersection issues in related areas such as anti-trust, and (iii) identify opportunities and mechanisms to collaborate, and to consider what form that collaboration would take.

Vehicles to achieve and complement the above include the holding of a cross-regulatory Workshop or Webinar to identify best practices on the conclusion of inter-agency agreements, information exchanges and joint enforcement actions.

### 3.2 STAKEHOLDERS

- Authority for Consumer & Markets – Netherlands (observer)
- Belgium DPA
- Datatilsynet Norway
- Datatilsynet Denmark
- EDPS
- FTC
- Information Commissioner's Office, United Kingdom
- National Privacy Commission, Philippines ("NPC")
- OAIC
- OPC Canada

### 3.3 OBJECTIVES

| NO | GOALS | OBJECTIVES | BUSINESS OUTCOMES |
|---|---|---|---|
| 1. | To continue the study of the overlap of substantive legislation affecting the rights of digital consumers | To map and analyze cases where there is an overlap between privacy, consumer protection, competition or anti-trust | Report to 2019 ICDPPC |
| 2. | To utilize and engage in networks that involve privacy, consumer protection or competition, and/or data protection | Reach out to authorities through networks such as GPEN, ICPEN, International Competition Network, the Digital Clearing House, and the European Consumer Protection Network to inform about the work of the DCCWG | Presentations and interventions at various international fora by DCCWG chair and members (engagements to be divided amongst members). |
| 3. | To arrange a workshop that allows for the identification of best practices when DPAs and Consumer Protection and/or Competition authorities are collaborating | Practical approach on understanding inter-agency cooperation and best practices | Workshop |

| NO | GOALS | OBJECTIVES | BUSINESS OUTCOMES |
|---|---|---|---|
| 4. | Report back to the 41st conference on objectives identified by the resolution and submit a further resolution. | To inform the ICDPPC about the work of the DCCWG for 2018-2019 | Presentation, Report |

## 4. MILESTONES

The table below lists the milestones for this project, along with their estimated completion timeframe.

| Milestones | Estimated Completion Timeframe | Completed | DPA(s) Responsible |
|---|---|---|---|
| Presentation of white paper at European Consumer Protection Network Workshop | November 23rd, 2018 | Completed | Belgium DPA |
| Presentation of white paper at Digital Clearing House | 10th December, 2018 | Completed | OPC |
| Workshop at GPEN Practitioner's Enforcement Event | 16 May 2019 | Completed | OPC, OAIC, NPC, FTC, ICO |
| Engage with Digital Clearing House network | 5th June, 2019 | Completed | OPC, EDPS |
| Attendance/Presentation at ICPEN | September 2019 | TBD | OPC |
| Prepare and table third DCCWG resolution | Due 26 August 2019 (with 4+ co-sponsors) | TBD | TBD |
| DCCWG Report for presentation at ICDPPC Conference | Due 26 August 2019 (with 4+ co-sponsors) | TBD | TBD |
| Report back to ICDPPC | 21-24 Tirana, Albania | TBD | OPC and OAIC |

# Appendix D: List of DCCWG Engagements

| Date | Conference | Topic | Location | Representative |
|---|---|---|---|---|
| 23 November 2018 | CPC (Consumer Protection Cooperation network)/EDPB joint workshop | DCCWG – White Paper | Brussels, Belgium | Belgium DPA |
| 3-4 December 2018 | 50th Asia Pacific Privacy Authorities | DCCWG – White Paper | Wellington, New Zealand | OPC |
| 10 December 2018 | 4rd Meeting of the Digital Clearing House | DCCWG – White Paper | Brussels, Belgium | OPC |
| 16-17 May 2019 | Global Privacy Enforcement Network – Enforcement Practitioner's Workshop | DCCWG – Workshop/Break Out Session | Macau, China | OPC, OAIC, FTC, NPC, ICO |
| 5 June 2019 | 5th Meeting of the Digital Clearing House | DCCWG – Questions for Network | Brussels, Belgium | OPC |
| 23-27 September 2019 | International Consumer Protection Enforcement Network | DCCWG – White Paper | Cartagena D.T., Colombia | OPC |

# Appendix E: GPEN Exit Note


3rd Annual GPEN Practitioner's Enforcement Workshop – MACAU, CHINA

MAY 17, 2019

# *Global Privacy Enforcement Network*

# *&*

# *Digital Citizen and Consumer Working Group*

# *Break Out Session on Cross Collaboration*

# *Summary of Discussion*

## THANK YOU

Thank you for your contributions to the break out session at the GPEN Practitioner's Workshop in Macau, China on the topic of the intersection between privacy and consumer protection/competition (and/or other authorities that cross regulate the digital economy). As indicated at the workshop, we have put together this summary in hopes to utilize and share information learned from the individual breakout sessions. Attached to this document at **Appendix A** is the list of questions that was distributed at the breakout session. Please feel free to send any further responses to april.gougeon@priv.gc.ca. On behalf of the *Digital Citizen and Consumer Working Group,* we'd like to thank GPEN, its co-hosts, the Office for Personal Data Protection, Macao and the Privacy Commissioner for Personal Data, Hong Kong, and the attendees of this conference for their valuable insights with regards to this topic.

## SUMMARY OF DISCUSSION

### COOPERATION WITH CONSUMER PROTECTION, COMPETITION OR OTHER RELEVANT AUTHORITIES

- Most DPAs are cooperating with consumer protection regulators on a policy level. This is not to say cooperation isn't also occurring at an enforcement level.
- One authority stated that it has extensive interaction with its consumer regulator and is expected to co-regulate proposed legislation on consumer rights (involving a right to data portability) with its consumer authority. If the legislation passes, a new system would be established where the DPA is expected to be the primary complaint-handler, with the responsibility of overseeing the privacy aspects of complaints, while the consumer regulator would be responsible for other aspects of the system and take systemic enforcement actions. This proposed regime is anticipated to allow the DPA and consumer authority to share information relevant to the other's regulatory and enforcement role.
- Some authorities had formal agreements with other non-DPA regulators and others did not. The lack of a formal agreement did not preclude cooperation on a policy level.
- We saw an example of a DPA and consumer authority working together via the publishing of consumer protection articles – if the article had an element of privacy, the DPA would provide comments from a privacy perspective on the articles.
- DPA's also indicated that they are participating in public consultations together with their consumer regulator.

- Some DPA's share information with their consumer protection counterpart in terms of publications and ongoing projects – information is exchanged informally and a formal agreement is not in place for this kind of sharing.
- In some cases, complainants are encouraged to complaint to both the consumer office and DPA.
- In one case, a DPA has access to a database of all consumer complaints filed and they meet with the consumer agency to discuss trend data.
- With respect to the intersection between privacy and competition, most authorities indicated that this connection was still in its primary stages, however, work is being done.
- For example, one DPA arranged training with its competition authority to enhance cross-agency knowledge of the law. In this case, the DPA gave training to members of the competition authority and vice-versa in order to create mutual familiarization of each other's laws.
- Some DPA's have MOUs with their competition counterparts.
- High-level meetings between the Commissioners of DPAs and Commissioners of competition authorities are occurring.
- One DPA mentioned that the practical experiential aspect of the intersection between competition and privacy needs further exploration, for example, an understanding of how personal information is considered when a high profile merger involving personal data is taking place.
- One DPA provides input to its competition regulator on ad hoc basis.
- One DPA works together with other agencies to issue joint administrative orders between the agencies, as well as having MOUs in place in order to litigate files of the DPA.
- A notable theme that was raised concerns the cooperation between DPA's and authorities responsible for cybercrime, cyber security and/or hackers.
- We saw examples of DPAs referring cases to the police, or working with the police in regards to crimes that involve personal information.
- It was raised that there are many similar aims of data security and data protection legislation.
- One agency has an agreement with its local policy authority, in that they will refer cases to police if they have a criminal element (i.e. the DPA does not pursue those cases) — the local police will provide regular updates of the handling of the case.
- Another DPA cooperates with its cyber authority on both an intelligence and enforcement level – conducting joint searches and seizures (also with the police) and by jointly taking cases through the court process.

- Another area where there were there was cross-sectoral cooperation was with domestic telecom regulators and elections offices.
- Some consumer and data protection authorities are in the same Ministry – the issue is the need to establish jurisdiction instead of doing joint investigations. In this case, there is a government policy where an individual can complain to either and it will be directed to the proper authority.

## BARRIERS / CHALLENGES

- Almost across the board, participants cited the inability to share information as a barrier to cooperation – in particular, where this information was subject to secrecy, confidentiality or commercially sensitive provisions.
- In some cases, forwarding information between agencies requires consent and/or approval.
- In some cases, it was cited that a legal amendment would be required to allow for information sharing.
- Jurisdictional challenges were cited as a barrier to cooperation, e.g., the ability to investigate when the controller or the data is outside the authority's jurisdiction.
- Timing – problems can arise where another authority may announce a case while the investigation is still ongoing for a cross-regulatory counterpart.
- Receipt of insufficient information.
- Asymmetrical enforcement powers where consumer/competition authorities have fining power and sanctions, and DPAs do not.
- May be a difference in priorities and focus between the agencies.
- Lack of a general obligation to cooperate with other public authorities.
- Sometimes, when referring cases to police agencies, it was difficult to achieve engagement.
- Establishing cooperation on cases where there is an overlapping jurisdiction in relation to cybercrime was cited as a challenge in several cases.
- May be political or cultural factors – privacy may be used as a barrier to sharing information with agencies also regulated by the DPA.
- Legal “grey areas” – use of evidence obtained in one case in another proceeding.
- “Forum shopping” – complainants filing complaints with multiple authorities where the DPA does not have sole jurisdiction.

## BEST PRACTICES, KEY LEARNINGS

- Have information sharing authorization in each agency's legislation to ensure that expertise and complaint/enforcement information can be shared.
- Need to consult where there is overlap and establish a mutual trust between regulators.
- Have a designated point of contact between authorities. Familiarity and trust is key, especially when dealing with agencies who may not take your case. Routine communication is crucial.
- Working collaboratively to ensure that all regulatory issues are identified and dealt with by the regulator with the appropriate expertise (with input from others as required).
- With collaboration, the key is to create an ease of doing business – to be able to pick up the phone and expedite concerns or complaints submitted.
- Information sharing agreements and MOUs are helpful.
- Sharing sufficient levels of information.
- Identifying challenges/hurdles to overcome and learning from experience.
- Joining mutually beneficial networks (for example, APEC.)
- International networks playing an active role – e.g., have an activity that gets these groups together in order to share practices and communicate. Leverage ICPEN, ICN, GPEN, and increase communication among networks.
- In some jurisdictions, the government has formalized a community of practice for all government regulators to share practices and experiences relating to competition or regulatory matters, which can help make cooperation effective.
- In another jurisdiction, there is a government policy that government agencies cannot turn a client down, and therefore, if complaints are received or issues are raised that are not in an agency's jurisdiction, referrals or endorsements are made to the proper authority.
- From a consumer perspective, dealing with the regulators should be 'seamless', i.e. a consumer who contacts one regulator to report an issue or make a complaint is not turned away and told to contact the other regulator.
- Deconfliction: in the case of cyber security (dealing with secure infrastructure), there is an overlap between personal data and the tools used for cyber security – for example, the point of view of the DPA might be to notify a target whereas the objective of cyber security may be to identify a hacker who is trying to obfuscate his identify. In this case, an MOU would be a best practice in order to deconflict.
- Fostering a culture of sharing and communication.
- Policy directions and statements can assist in helping authorities to communicate both at a national and international level.

- Both privacy and consumer protection regimes have a role to play in regulating multi-faceted issues – privacy regulators should share their knowledge and expertise in applying privacy law with others.
- A practical benefit is that initiatives that may promote competition may also have significant privacy implications as well as broader consumer protection issues – given this cross-over, there are clear benefits in involving all regulators in order to ensure the appropriate expertise is available for handing all regulatory issues that arise.
- Privacy education and awareness through consumer groups.
- Engagement at Commissioner level.
- It is useful to have common understandings of material elements (such as consent) when discussing with competition or consumer regulator.

## SUBSTANTIVE OVERLAPS

- A few DPAs indicated there was an overlap in jurisdiction – for example, proposed legislation in one country would assign regulatory compliance to both the DPA and consumer agency with respect to consumer rights, such as data portability.
- Several DPAs answered that there is no overlap but instead common legal issues concerning data protection and unfair trade practices. Some cases will raise issues for both privacy and consumer protection – statutes don't exclude each agency from pursuing.
- Some authorities stated that an overlap can occur in practice, for example, in cases of telemarketing, spam, data breaches, e-commerce, and other cases involving the collection and use of data.
- Some DPAs mentioned that many common legal issues arise where competition cases involve technology (i.e. merger of tech companies with personal data as assets).
- One DPA indicated that they meet with their consumer authority on issues surrounding credit reporting.
- Several DPA's also mentioned that common legal issues arise between them and their domestic cyber security regulators.

## APPENDIX A

### Questions for Breakout Session on Cross Collaboration

1. Do you or your agency cooperate either domestically or internationally with agencies other than data protection agencies (DPAs)? What has been your experience with competition and/or consumer regulators (or others)? (e.g. no interaction/interaction at a policy level/interaction at an enforcement level – please provide examples.)

   a. In your opinion or experience, what are some best practices for cross-regulatory cooperation? Is there anything in particular that makes such cooperation effective?

   b. Are there any barriers to cross-regulatory cooperation or collaboration?

   c. Does your agency have any interagency agreements in place with authorities other than DPAs? What is the preferred approach (formal vs informal)?

d. What have been the key learnings for you in collaborating with competition, consumer or other non-DPA regulators in your jurisdiction?

2. Does your domestic consumer protection or competition agency have any overlaps in jurisdiction with privacy or data protection? Are there any common legal issues?

   a. In what particular substantive areas have there been synergies? E.g. collection, consent, fairness.

3. Have you had experiences where a matter in your jurisdiction has been pursued by agencies in different realms? If so, describe what challenges and/or opportunities that raised.

# Appendix F: DCH Exit Note


5th Annual Meeting of the Digital Clearinghouse – BRUSSELS, BELGIUM

5TH JUNE 2019

# *Digital Citizen and Consumer Working Group – Summary of Responses from Members of the Digital Clearinghouse*

## THANK YOU

Thank you for your contributions and responses to the questions distributed by the *Digital Citizen and Consumer Working Group* (DCCWG) at the 5th annual meeting of the Digital Clearinghouse in Brussels, Belgium on the topic of the intersection between privacy and consumer protection/competition on the 5th of June, 2019. The DCCWG has put together this brief summary of your responses in hopes to utilize and share information learned from the responses to the questions. On behalf of the DCCWG, we'd like to thank the Digital Clearinghouse, and its hosts, Dr. Alexandre de Streel from the University of Namur, Dr. Inge Graef from the Tilburg University, the European Policy Centre and the attendees of this meeting for their valuable insights with regards to this topic.

## RESPONSES TO QUESTIONS

- We received a paper titled: *Long Term Impact of Big Tech Sector Mergers: a proposal of specific cooperation mechanisms between competition authorities and data protection authorities*, which is available online[1] and attached at Appendix A. This paper was written by authors from the Catalan Competition Authority Director General and the Competition and Consumer Protection Commission (Ireland) and finds that there is scope for data protection authorities and competition authorities to collaborate on issues derived from data infringements and competition law infringements.

- The following chart outlines the questions sent to members of the Digital Clearinghouse and provides a summary of the responses received:

[1] http://acco.gencat.cat/web/.content/80_acco/documents/arxius/actuacions/20180130_Long-Term-Impact-of-Big-Tech-Sector-Mergers-2.pdf

| No. | Questions | Responses |
|---|---|---|
| 1. | **What has been your experience cooperating, on either a domestic or international level, with agencies in a different regulatory sector? For example, if you are a data protection agency, what has been your experience with competition and/or consumer regulators (or others) and vice versa? (e.g. no interaction / interaction at a policy level / interaction at an enforcement level – please provide examples.)** | • One Data Protection and Privacy Authority ("DPA") stated that it has limited experience in cooperating with other national regulators;<br>• Occasionally this DPA has received some questions coming from ministries responsible for consumer protection law enforcement on the precise interpretation of privacy regulation on a specific question;<br>• This has not yet led to a form of institutionalized cooperation or joint enforcement operations.<br>• One consumer protection authority mentioned it had several formal partnerships with other authorities, involving formal cooperation protocols. These formal cooperation protocols contain the engagement to meet at least annually on common issues.<br>• This consumer authority also indicated that nationally both consumers and companies are able to report issues or file complaints regarding various government competences via a |

| No. | Questions | Responses |
|---|---|---|
| | | common web portal, which automatically shares the complaint with the competent agency.<br><br>• One competition authority indicated that it cooperates with market regulators in the telecommunications, banking, and energy and water sectors, as well as with all other regulators when investigating markets or giving regulatory recommendations after the evaluation of the legal frameworks in force.<br>• With almost all of these regulators, the competition authority signs Memorandums of Understanding ("MOUs") where both parties agree to cooperate and exchange the relevant data.<br>• In particular, this competition authority indicated that it is a priority for its Office to complete an MOU with its domestic DPA(s).<br>• This authority also indicated that is has authority with regards to a regulation on the protection, processing, storage and security of personal data. |
| 2. | **In your opinion or experience, what are some best practices for cross-regulatory cooperation? Is there anything in particular that makes such cooperation effective?** | • Some best practices were cited as:<br>○ MOUs;<br>○ Having a legal framework for cooperation and concluding formal protocols as a firm base for cross-regulatory cooperation; |

| No. | Questions | Responses |
|---|---|---|
| | | ○ The organization of mutual workshops;<br>• Formal protocols are no guarantee for practical success – as such cooperation can also be started in an informal way, for example, by talking about shared issues, formulating shared guidance, and agreeing on who will investigate a specific sector practice.<br>• Set up a minimal cooperation framework first, before delving into actual joint enforcement. Even though such a framework would not be able to anticipate nor resolve all the questions that would inevitably flow from a concrete enforcement case, it can help to put in place a more systematic and regular exchange of information. Such exchanges help in building trust between authorities and eventually taking the next step to joint enforcement. |
| 3. | **Are there any barriers to cross-regulatory cooperation or collaboration?** | • One consumer authority cited that their agents have a duty of professional secrecy and as such, they cannot share confidential information with other persons or authorities. However, a specific exception exists for sharing information with other public authorities if this is part of the investigation, prosecution and sanctioning of infringements within their competence. Furthermore this agency has the specific power to request that all State services collect and provide any information and documents that are considered useful for the performance of their duties.<br>• One competition authority indicated that there are no barriers to cross-regulatory collaboration, citing a regulatory impact |

| No. | Questions | Responses |
|---|---|---|
| | | assessment which states that on competition protection/market surveillance matters, the competition authority is a regulator above the regulators.<br>• One DPA stated that although they have not yet had in-depth policy discussions with other regulators on more advanced cooperation, no preliminary discussions have raised specific issues that could bar cooperation. In particular, their domestic legislation explicitly provides for the possibility of cooperation. The legislation allows the DPA to:<br>o Act in the spirit of dialogue with all relevant actors, including government actors, and take into account the interests of consumers;<br>o Act upon the request or assistance of other national authorities;<br>o Conclude protocols with third parties with regards to confidentiality obligations in order to exchange necessary information. |
| 4. | **Does your domestic consumer protection or competition agency have any overlaps in jurisdiction with privacy or data protection? Are there any common legal issues? In what particular substantive areas have there** | • One competition authority stated there are no overlaps— each institution is based on its law has its own mission and duties.<br>• One consumer authority stated they do not have formal privacy or data protection powers, however, they do have some "overlaps" where they may tackle a shared issue from a different angle. For example, this is mostly done via pre-contractual information |

| No. | Questions | Responses |
|---|---|---|
| | **been synergies? E.g. collection, consent, fairness.** | obligations, the obligation of professional diligence, and unfair commercial practices and unfair contract terms. For example, within the European Consumer Protection Cooperation network, European consumer authorities asked Facebook to change and clarify some of its terms & conditions (http://europa.eu/rapid/press-release_IP-19-2048_en.htm).<br>• One DPA stated that they are aware of the broader ongoing discussions on this topic, and that overlaps are present, but are still in the process of charting substantive overlaps in dialogue with its consumer and competition counterparts. |

# Appendix A

# Long Term Impact of Big Tech Sector Mergers:
## A proposal of specific cooperation mechanisms between competition authorities and data protection agencies[1]

### 1.- The Digital Clearing House initiative

The European Data Supervisor announced in September 2016[2] his intention to set up a Digital Clearing House initiative to explore the possibilities of improving the cooperation between regulators as an adequate response to the "*concentration of market power and personal data in fewer and fewer hands*" and consider that "*Data protection, consumer and competition law each in theory serve common goals, but in reality they generally work in silos, according to the EDPS*".

Following on from this, we believe that the Digital Clearing House may wish to explore specific cooperation mechanisms between Competition Authorities and Data Protection Agencies to progress this discussion.

### 2.- Cooperation mechanisms

Cooperation between data protection agencies and competition authorities could be two-way depending on the area of work involved.

- **Big Tech Sector Mergers**

**Monitor merger conditions in terms of data imposed by competition authorities (competition -> data protection)**

In recent years, we have witnessed a number of Big Tech sector mergers[3] as the world becomes more digitised than ever. At the centre of these mergers is the acquisition and consolidation of large volumes of data, otherwise known as Big Data. The value of Big Data has increased exponentially in recent times as new uses such as generating artificial intelligence (AI) and "cognitive" services have been identified.[4] These services are sold to other businesses and utilised in the production and sale of their own products. This has developed a number of new revenue streams for so-called "data brokers" in the expanding "data economy".

[1] Authors: Marc Realp (Catalan Competition Authority Director General) & Xavier Puig (Catalan Competition Authority) & Emily Thornton (Competition and Consumer Protection Commission (Ireland)). Disclaimer: The views and opinions expressed in this paper are those of the authors and do not necessarily reflect the official policy or position of the aforementioned competition authorities.

[2] Statement: The coherent enforcement of fundamental rights in the age of Big Data. 23 September 2016. https://edps.europa.eu/press-publications/press-news/press-releases/2016/statement-coherent-enforcement-fundamental-rights_en ; Opinion 8/2016. EDPS Opinion on coherent enforcement of fundamental rights in the age of big data. 23 September 2016. https://edps.europa.eu/sites/edp/files/publication/16-09-23_bigdata_opinion_en.pdf

[3] For instance, COMP/M.7217 – Facebook/WhatsApp which can be accessed at: http://ec.europa.eu/competition/mergers/cases/decisions/m7217_20141003_20310_3962132_EN.pdf and Case M.8124 –Microsoft / LinkedIn which can be accessed at: http://ec.europa.eu/competition/mergers/cases/decisions/m8124_1349_5.pdf

[4] "Data is giving rise to a new economy", The Economist. Please see: https://www.economist.com/news/briefing/21721634-how-it-shaping-up-data-giving-rise-new-economy

Facebook-WhatsApp

The acquisition and consolidation of large volumes of data was one aspect of the Facebook-WhatsApp merger[5] - assessed by the European Commission. The European Commission analysed potential data concentration issues only to the extent that they could impede competition in the online advertising market, whilst also segmenting privacy issues and merger control.[6] The European Commission stated in a press release that, "*any privacy-related concerns flowing from the increased concentration of data within the control of Facebook as a result of the transaction do not fall within the scope of EU competition law*".[7] In contrast, it has also been noted by the US Federal Trade Commission[8] that mergers may adversely affect non-price parameters for competition such as consumer privacy.[9]

Microsoft-LinkedIn

In the Microsoft-LinkedIn merger, the European Commission analysed merger-specific potential data concentration relating to the potential impact on competition in the Single Market.[10] The European Commission emphasised privacy as a quality metric in their assessment, noting that privacy-related concerns "*can be taken into account in the competition assessment to the extent that consumers see it as a significant factor of quality*". The European Commission concluded that data privacy was an important parameter of competition between professional social networks on the market. As such, the European Commission imposed proportionate and relevant remedies on the merging parties to prevent this parameter from being negatively affected by the transaction.

These two mergers have demonstrated that data protection and privacy issues have come to the forefront of Big Tech mergers. Therefore, it is becoming necessary for National Competition Authorities to ensure that a consistent approach is adopted in reviewing mergers involving Big Tech sectors. Furthermore, closer cooperation with data protection regulators may be necessary.

Big Data mergers present competition authorities with a number of unique and novel issues to consider, e.g., procedural issues and relevant market definition issues. This has prompted the Directorate General for Competition ("DG Comp") to issue a "*Consultation on Evaluation of procedural and jurisdictional aspects of EU merger control*".[11] Following on from this, the German Parliament introduced, among other

[5] Case No COMP/M.7217 – Facebook/WhatsApp http://ec.europa.eu/competition/mergers/cases/decisions/m7217_20141003_20310_3962132_EN.pdf
[6] Case No COMP/M.7217 – Facebook/WhatsApp. Please see: http://europa.eu/rapid/press-release_IP-14-1088_en.htm
[7] Case No COMP/M.7217 – Facebook/WhatsApp. Please see: http://europa.eu/rapid/press-release_IP-14-1088_en.htm
[8] Please see Statement of Federal Trade Commission concerning their assessment of the Google-Double Click transaction which can be accessed at: https://www.ftc.gov/system/files/documents/public_statements/418081/071220googledc-commstmt.pdf
[9] It has been argued that consumers give their personal data to companies in return for the free use of their services (e.g, communication services, networking services, etc). In this sense, privacy is in effect the price they pay to avail of these free services.
[10] Case M.8124 –Microsoft / LinkedIn which can be accessed at: http://ec.europa.eu/competiti
[11] http://ec.europa.eu/competition/consultations/2016_merger_control/index_en.html

changes, a "*size of transaction test*" in merger control[12] to better capture "*data mergers*" in the relevant legislation. Similarly, the Austrian Competition Act was amended to include a new "*transaction value test for merger control*" that "*aims to cover cases with respect to the acquisition of start-ups in the digital economy, where the target has little to no current turnover and is bought primarily because of its potential growth*".[13]

Another recurring issue is the relevant market definition in a "data merger" (i.e., mergers where data is considered an essential asset). It could be argued that, the relevant market definition ought to take into consideration the multiple uses which the data may present in the future. These additional uses would pose a small cost on the relevant data undertaking and as such, is quite different from brick and mortar businesses where for example transforming a car factory into a shoe factory would impose significant costs and structural changes on the relevant undertaking. It may be near impossible for competition authorities to foresee and thus assess the complete range of future uses derived from a data merger. Therefore, it may be necessary to limit the merger clearance to the initial scope of the data merger. This may limit the risk of competition authorities accidentally omitting a potential market from their merger assessment. Post-transaction, if the merged parties were to enter a "new" data-related market which is beyond the initial scope of the merger, the relevant competition authority may wish to reassess the merger under these circumstances. Of course, this may limit the legal certainty of the merger clearance. At the same time, there is also a risk that competition authorities may not foresee future developments of the data economy. Therefore, it may be necessary that the market definition is *always* limited as a condition for data mergers which are cleared, otherwise, it may be impossible for competition authorities to assess the complete range of future implications deriving from a data merger.

It may also be the case that competition authorities clear a data merger by imposing data related conditions, e.g., allowing portability or providing direct access to third parties.

It could be argued that, data protection authorities are best placed to assess whether the relevant market condition or the data related conditions are being respected by the relevant undertakings post-transaction. This is comparable to when a data protection authority must determine whether an undertaking which has obtained a user's data has respected the scope for which the undertaking had obtained the user's consent.

Data protection authorities ought to alert the relevant competition authority if one of the data related conditions is not appropriately implemented or there is a breach of the conditions by the relevant undertaking, post-transaction. Therefore, it is necessary to build mechanisms that will enable data protection authorities and competition authorities to improve cooperation. In this case the mechanism should make it possible for the competition body to send all relevant information to the data protection agency. This will enable the data protection agency to appropriately monitor the data-related conditions imposed on the undertaking by the competition authority. It should

[12] Germany: Ninth Amendment of the Act against Restraints of Competition enters into force. Freshfields Bruckhaus Deringer. 9 June 2017. http://knowledge.freshfields.com/en/Global/r/3511/germany__ninth_amendment_of_the_act_against_restraints_of

[13] Schönherr. 6 April 2017. https://www.schoenherr.eu/publications/publications-detail/significant-amendments-to-austrian-competition-law-part-i-overview/

be noted that several competition authorities have established similar cooperation mechanisms with specific sector regulators when evaluating mergers in regulated sectors.

- **Data privacy infringements**

**Potential antitrust infringement deriving from a prior data violation (data protection -> competition)**

Competition Authorities have a legal mandate to protect the competitive environment and as such safeguard consumer welfare. The welfare notion includes not only the price element, but also the number of products offered, their variety and their quality. In this context, qualitative variables include personal data privacy, an element which can also be conceived of as a non-monetary price.

As the Facebook Bundeskartellamt case shows, an antitrust infringement deriving from a prior data violation is conceivable. In this case, the data violation is evaluated as a potential abuse of dominant position.

The underlying idea is that a breach of the relevant Data Regulation must be proven prior to initiating an antitrust investigation. This could be the minimum quality threshold for an antitrust investigation of this nature. As such, it could be argued that a violation of the relevant data regulation may also be considered as an exploitative abuse in terms of the quality of the goods or services offered.

Therefore, it must first be determined whether there has been an infringement of data protection regulation (either national or the EU General Data Protection Regulation – GDPR) and only afterwards, whether the issue can also be considered as an antitrust violation. In this sense, it is worth ensuring that there is an effective coordination mechanism between both agencies so that competition authorities are notified when a data protection issue may also be of interest from an antitrust perspective.

This coordination will allow competition authorities to understand the types of data infringements carried out by undertakings with substantial market power and the potential infringements which may substantially benefit the infringing party and thus strengthen a relevant market position.

Of course, it must be noted that not all data infringements attributable to a potential dominant firm may encompass an antitrust infringement (for example, not adequately securing data will probably never make it to an antitrust infringement). Therefore, it may be the case that only those data infringements which provide a significant benefit to the infringing party may fall within the scope of antitrust.

In summary, data protection authorities could support the work of competition authorities by alerting them of potential antitrust infringements in terms of data. Therefore, data protection authorities and competition authorities could set up mechanisms for data protection authorities to share all relevant material so that antitrust authorities can assess the possibility of initiating a competition proceeding.

The next step in this area could be to identify GDPR infringements which could potentially be considered as an antitrust infringement. This task may assist future

guidelines on when and how data protection authorities should notify competition authorities.

**EU General Data Protection Regulation ("EU GDPR") breaches which could potentially be considered as an antitrust infringement…**

Article 25 of the EU GDPR illustrates the requirements on data controllers to implement privacy by design and privacy by default on their systems.[14] In practise, privacy by design means that any business department which processes personal data must ensure that privacy and data protection is built into a system from the offset and during the entire life cycle of the system or process.[15] This includes internal projects, product development, software development, IT systems, etc. This will change the common practise of tagging security or privacy features at the end of a long production process.[16] Privacy by default demonstrates that once a product or service has been released to the public, the strictest privacy settings should apply by default, without any manual input from the end user.

It could be argued that a breach of Article 25 of the EU GDPR could potentially translate into a potential antitrust infringement such that a dominant player fails to implement privacy by design or privacy by default and consumers have no alternative privacy option.[17] For instance, this may be relevant in such circumstances where consumers see privacy as a significant factor of quality and thus translates into a direct or indirect reduction of consumer welfare.

## 3.- Conclusion

We believe that there is scope for data protection authorities and competition authorities to collaborate on the issues raised in this paper. Competition authorities may benefit from observing data protection authorities work and understanding the issues derived from data infringements which may also infringe on provisions of competition law. Furthermore, data protection authorities may also have a role on data mergers by monitoring data related conditions imposed on the merging parties.

Let's explore those possibilities together!

October 2017

[14] Please see https://gdpr-info.eu/art-25-gdpr/
[15] "What is Privacy by Design & Default?", which can be accessed at: https://www.ics.ie/news/what-is-privacy-by-design-a-default
[16] "What is Privacy by Design & Default?", which can be accessed at: https://www.ics.ie/news/what-is-privacy-by-design-a-default
[17] This could also potentially breach Consumer Protection Laws.

# Appendix G: Mapping Initiatives

| Jurisdiction | Development type | Details |
|---|---|---|
| United States of America | - Policy (domestic) | **Public Hearings on issues related to Competition and Consumer Protection in the 21st Century**<br><br>The Federal Trade Commission 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.<br><br>Many of the hearings intersected with privacy (Hearing 6 – Privacy, Big Data and Competition;[1] Hearing 9 – Data Security;[2] Hearing 12 – The FTC's Approach to Consumer Privacy[3]). |
| United States of America | - Laws and Instruments | **Federal Trade Commission**<br><br>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. |
| Canada | - Policy (domestic) | **Discussion paper considering Big Data and Competition Policy**<br><br>In 2017, the Canadian Competition Authority (the Competition Bureau) released its discussion paper 'Big Data and Innovation: Implications for Competition Policy in Canada'. The Canadian Data Protection Authority (the Office of the Privacy Commissioner) provided a submission and welcomed the |

[1] https://www.ftc.gov/news-events/events-calendar/ftc-hearing-6-competition-consumer-protection-21st-century
[2] https://www.ftc.gov/news-events/events-calendar/ftc-hearing-competition-consumer-protection-21st-century-december-2018
[3] https://www.ftc.gov/news-events/events-calendar/ftc-hearing-competition-consumer-protection-21st-century-february-2019

| Jurisdiction | Development type | Details |
|---|---|---|
| | | opportunity to engage in a meaningful dialogue with the Competition Bureau on the challenges relating to the collection, use, and disclosure of personal information in Big Data.[4]<br><br>In 2018, the Competition Bureau released a summary of key themes revealed in its consultation process. In respect of privacy, the Competition Bureau notes that there are potential overlapping enforcement activities under Canada's competition and privacy law.[5]<br><br>In 2019, the Competition Bureau 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. |
| Australia | - Policy (domestic) | **Government inquiry into Digital Platforms**<br><br>The Australian Government tasked the Australian Competition Authority (the Australian Competition and Consumer Commission (ACCC)) with undertaking an Inquiry into the practices of Digital Platforms.<br><br>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 Australian Data Protection Authority (the Office of the Australian information Commissioner (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.[6] |
| Australia | - Law and instruments | **Legislative development with dual role for competition authority and data protection authority**<br><br>Australia is currently developing a national Consumer Data Right (CDR). This initiative aims to give consumers greater control over how their data is used and disclosed to create more choice and |

[4] https://www.priv.gc.ca/en/opc-actions-and-decisions/submissions-to-consultations/sub_cb_171117/#fn6
[5] https://www.competitionbureau.gc.ca/eic/site/cb-bc.nsf/eng/04342.html
[6] https://www.oaic.gov.au/engage-with-us/submissions/digital-platforms-inquiry-preliminary-report-submission-to-the-australian-competition-and-consumer-commission

| Jurisdiction | Development type | Details |
|---|---|---|
| | | competition. It is a right to allow consumers to access particular data in a readily usable form, and to direct a business to securely transfer that data to an accredited third-party data recipient.<br><br>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.<br><br>Under the proposed legislation both the Australian Data Protection Authority (the Office of the Australian information Commissioner (OAIC)) and the Australian Competition Authority (the Australian Competition and Consumer Commission (ACCC)) will oversee the CDR under a co-regulator model. The OAIC will regulate the privacy aspects of the scheme, provide 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. |
| Singapore | - Policy (domestic) | **Research into data portability**<br><br>The Singaporean Data Protection Authority (the Personal Data Protection Commission) released a Discussion Paper on Data Portability. The paper provides a framework for stakeholders to discuss data portability and generate feedback for future consultations to determine the optimal approach, and was developed in collaboration with the Singaporean Competition Authority (the Competition and Consumer Commission of Singapore). |
| Philippines | - Policy (domestic) | **Development of advisories and papers on the protection of personal information of digital consumers**<br><br>The Philippines' National Privacy Commission (NPC) is currently developing advisories and working papers that aim to address the needs of data subjects who are engaged in online transactions, sharing or disclosure of personal data for business operations and the use of portable storage devices. Due to the |

| Jurisdiction | Development type | Details |
|---|---|---|
| | | exponential growth of online transactions in the Philippines, the NPC initiated the development of these guidelines to aid data subjects, as consumers and stakeholders of digital platforms to exercise due care and caution in engaging with business operators online which involve the collection and processing of personal data. The documents that the NPC is working on are the following: Guidelines for unsolicited promotional messages, Guidelines to Outsourcing Agreements, Advisory on Direct Marketing, Guidelines on processing personal information for loan related transactions, Advisory on the use of Portable Storage Devices. These materials will be available on] the website of the NPC by the end of the year. |
| Philippines | - Policy (domestic) | **Mobile Application Assessment**<br><br>As consumers in the Philippines heavily rely on digital platforms for their daily transactions, the NPC initiated an on-going project entitled "Mobile Application Assessment" which aims to evaluate the permissions and terms and conditions of both local and international mobile applications which collect personal data. To date, there have been two hundred (200) applications assessed. The objective of the project is to detect applications that have no privacy notices, direct the improvement of privacy policies, and impose collection of relevant personal data only. For the consumers, the project intends to provide guidance on the aspects that the users shall consider before engagement and the extent of personal data to be disclosed. |
| Norway | - Policy (domestic) | **Common Framework between Data Protection authority, Consumer Protection authority and Consumer Council**<br><br>The Norwegian Data Protection Authority (Datatilsynet), the Norwegian Consumer Protection Authority (Forbrukertilsynet) and the Norwegian Consumer Council (Forbrukerrådet) have seen the importance of working together to strengthen consumer rights in the digital economy. The authorities have developed |

| Jurisdiction | Development type | Details |
|---|---|---|
| | | close co-operation on policy and enforcement issues. The data and consumer protection authorities have drawn 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. |
| Norway | - Enforcement | **Co-ordination of an enforcement case between data protection authority and consumer protection authority**<br><br>The Norwegian Consumer Council (Forbrukerrådet) has analyzed terms and conditions in so-called "smart products" such as fitness trackers, toys, health apps and GPS watches. Their analysis shows that there are major challenges related to data security when it comes to “Internet of things” devices.<br><br>In 2017, the Consumer Council conducted an investigation into the security of various types of GPS watches marketed to children. The investigation showed that it was possible for unauthorized persons to extract information from the watch, as well as to read and change its location data. It was also possible to link the watch to a new account without the owner’s knowledge. These shortcomings constituted several breaches of European data and consumer protection laws.<br><br>In the wake of their findings, the Consumer Council submitted complaints regarding three GPS watches to the data protection authority and the consumer protection authority. These two authorities addressed the cases in co-ordination. Case handlers from both authorities worked together in order to make preliminary assessments of the cases and to outline the main concerns pursuant to the authorities’ respective legal frameworks.<br><br>The data protection authority (Datatilsynet) decided, after assessing the cases, to order the three controllers to cease processing of all personal data relating to the GPS watches due to poor security of processing. As a result of this order, one of the three data controllers decided to terminate its services. In the remaining two cases, the consumer protection authority (Forbrukertilsynet) also made their own |

| Jurisdiction | Development type | Details |
|---|---|---|
| | | assessments, however, those assessments did not substantially concern the intersection of consumer and data protection. |
| Netherlands | - Laws and Instruments | **Collaboration Agreement between Data Protection Authority and Consumer Protection Authority**<br><br>In 2016, the Dutch data protection authority (Autoriteit Persoonsgegevens) and the Dutch consumer protection and competition authority (Autoriteit Consument en Markt) concluded a collaboration agreement to clarify the procedures to follow in case their respective competencies overlap or intersect.[7] The collaboration agreement states explicitly that concluding such an agreement has both the benefit of avoiding ad hoc agreements for each separate case and also establishing a co-operation framework that is transparent to all stakeholders.<br><br>The collaboration agreement formalizes some co-ordination mechanisms such as a yearly meeting on their ongoing co-operation, the designation of a distinct contact person within each authority and an evaluation of its functioning every three years. In addition, the agreement provides for information exchange and co-operation in case of concurrent competencies. |
| United Kingdom | - Policy (domestic) | **Government inquiry into Ad Tech**<br><br>In July 2019, the UK Competition Authority (the Competition and Markets Authority (CMA)) launched a market study into online platforms and the digital advertising market in the UK. The CMA is assessing three broad potential sources of harm to consumers in connection with the market for digital advertising:<br><br>- to what extent online platforms have market power in user-facing markets, and what impact this has on consumers |

[7] ACM & AP, "Samenwerkingsprotocol tussen Autoriteit Consument en Market en Autoriteit Persoonsgegevens", *Staatscourant* 3 November 2016, https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/convenant_acm-ap.pdf

| Jurisdiction | Development type | Details |
|---|---|---|
| | | - whether consumers are able and willing to control how data about them is used and collected by online platforms<br><br>- whether competition in the digital advertising market may be distorted by any market power held by platforms.[8]<br><br>This Study has come after the UK Data Protection Authority (Information Commissioner's Office (ICO)) published a report on its own research into advertising technology and real-time bidding. The report found that the Adtech industry needed to make improvements to comply with the law and set out expectations around actions to be taken and the timeframes to be achieved.[9] |
| France and Germany | - Policy (regional) | **Joint report between German and French competition authorities considering intersection between data protection and competition laws**<br><br>In May 2016, the German Competition Authority (Bundeskartellamt) and French Competition Authority (Autorité de la concurrence) wrote a joint report on the role of data in economic relationships as well as in the application of competition law to such relationships. In this report they identified some intersections between data protection and competition law:<br><br>*"Indeed, even if data protection and competition laws serve different goals, privacy issues cannot be excluded from consideration under competition law simply by virtue of their nature. Decisions taken by an undertaking regarding the collection and use of personal data can have, in parallel, implications on economic and competition dimensions. Therefore, privacy policies could be considered from a competition standpoint whenever these policies are liable to affect competition, notably when they are implemented by a dominant undertaking for which data serves as a main input of its products or services. In those cases, there may be a close link* |

[8] https://www.gov.uk/cma-cases/online-platforms-and-digital-advertising-market-study
[9] https://ico.org.uk/media/about-the-ico/documents/2615156/adtech-real-time-bidding-report-201906.pdf

| Jurisdiction | Development type | Details |
|---|---|---|
| | | *between the dominance of the company, its data collection processes and competition on the relevant markets, which could justify the consideration of privacy policies and regulations in competition proceedings".*[10] |
| Germany | - Law and instruments<br>- Enforcement | **Competition authority decision using Data Protection laws**<br><br>In February 2019, the German competition authority (Bundeskartellamt) found that Facebook's terms of service and the manner and extent to which it collects and uses data are in violation of the European data protection rules to the detriment of users. The Bundeskartellamt closely cooperated with leading data protection authorities in clarifying the data protection issues involved. In the authority's assessment, Facebook's conduct represents above all a so-called exploitative abuse.[11]<br><br>The Bundeskartellamt's decision prohibits Facebook from collecting then combining user data from different sources without voluntary consent. Facebook has 12 months to discontinue its current practice of combining data from 3rd party sources with Facebook data, without voluntary consent. |
| Catalan and Ireland | - Policy (regional) | **Joint paper between Competition Authorities**<br><br>In October 2017, the Catalan Competition Authority (Autoritat Catalana de la Competència) and the Irish Competition Authority (Competition and Consumer Protection Commission) published a joint paper proposing the Digital Clearing House consider exploring specific cooperation mechanisms between data protection authorities and competition authorities, including: |

[10] Bundeskartellamt and Autorité de la concurrence, 'Competition Law and Data' (2016) http://www.autoritedelaconcurrence.fr/doc/reportcompetitionlawanddatafinal.pdf

[11] https://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2019/07_02_2019_Facebook.html

| Jurisdiction | Development type | Details |
|---|---|---|
| | | - Big Tech sector mergers: monitor merger conditions in terms of data imposed by competition authorities<br>- Data Privacy infringements: potential antitrust infringement deriving from a prior data violation<br>- EU GDPR breaches which could be considered an antitrust infringement.[12] |
| OECD Economies | - Policy (international) | **Recommendation concerning cooperation between data protection and consumer protection authorities**<br>In 2007, the OECD issued a recommendation containing several features which could facilitate co-operation between privacy and consumer protection authorities. Focusing on "Laws Protecting Privacy" (meaning "national laws or regulations, the enforcement of which has the effect of protecting personal data consistent with the OECD Privacy Guidelines"), it recommends that countries "improve their domestic frameworks for privacy law enforcement to better enable their authorities to co-operate with foreign authorities." Specifically, the OECD recommends that: data protection or privacy authorities be given mechanisms to share relevant information with foreign authorities relating to possible violations of laws protecting privacy; and data protection or privacy authorities be able to provide assistance to foreign authorities (relating to possible violations of their law protecting privacy), with regard to obtaining information from persons; obtaining documents or records; or locating or identifying organisations or persons involved.[13] |
| OECD Economies | - Policy (international) | **Going Digital project** |

[12] http://acco.gencat.cat/web/.content/80_acco/documents/arxius/actuacions/20180130_Long-Term-Impact-of-Big-Tech-Sector-Mergers-2.pdf

[13] http://www.oecd.org/internet/ieconomy/38770483.pdf

| Jurisdiction | Development type | Details |
|---|---|---|
| | | The OECD launched the 'Going Digital' project which is about giving policymakers the tools they need to help economies and society proposer in an increasingly digital and data-driven world.[14]<br><br>The OECD recognises that digital transformation affects many aspects of the economy and society in complex and interrelated ways, challenging existing policies in many areas. As a result, silos are disintegrating, and governments must strengthen both internal and external collaboration, and re-think about how policy is developed and implemented.[15]<br><br>The project draws on national experiences and policy experimentation occurring across OECD members, and seeks to share these experiences to assist countries in implementing an integrated policy approach to the digital transformation.[16]<br><br>Topics involving the intersection of privacy and competition include Digital Security and Privacy, Artificial Intelligence and Digital Consumers.[17] |
| OECD Economies | - Policy (international) | **OECD discussions**<br><br>The OECD has hosted numerous discussions on the intersection of privacy and competition, including:<br><br>- 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.[18] |

[14] https://www.oecd.org/going-digital/
[15] https://www.oecd.org/going-digital/framework/
[16] https://www.oecd.org/going-digital/project/
[17] https://www.oecd.org/going-digital/topics/
[18] http://www.oecd.org/daf/competition/conference-on-competition-and-the-digital-economy.htm

| Jurisdiction | Development type | Details |
|---|---|---|
| | | - In November 2018, the OECD Consumer Protection and Competition committees jointly discussed the ambiguous and multi-dimensional effects of personalised pricing.[19]<br><br>- In November 2016, the OECD held a hearing discussion on Big Data to explore the implications on competition authorities' work and whether competition law is the appropriate tool for dealing with issues arising from the use Big Data.[20] |
| European Union | - Policy (international) | **Digital Clearinghouse**<br><br>The European Data Protection Supervisor established the Digital Clearinghouse in May 2017.<br><br>The Digital Clearinghouse brings together agencies from the areas of competition, consumer and data protection willing to share information and discuss how best to enforce rules in the interests of the individual.[21]<br><br>All regulators in the digital space, based in the EU or around the world, are invited to take part in discussions hosted by the Clearinghouse.[22] |
| ICPEN/GPEN | - Enforcement | **The International Consumer Protection Enforcement Network and the Global Privacy Enforcement Network**<br><br>The International Consumer Protection Enforcement Network (ICPEN) is a membership organisation consisting of consumer protection law enforcement authorities from across the globe.[23] ICPEN provides a |

[19] https://www.oecd.org/daf/competition/personalised-pricing-in-the-digital-era.htm
[20] https://www.oecd.org/daf/competition/big-data-bringing-competition-policy-to-the-digital-era.htm
[21] https://edps.europa.eu/data-protection/our-work/subjects/big-data-digital-clearinghouse_en
[22] https://edps.europa.eu/data-protection/our-work/subjects/big-data-digital-clearinghouse_en
[23] https://www.icpen.org/who-we-are

| Jurisdiction | Development type | Details |
|---|---|---|
| | | forum for developing and maintaining regular contact between consumer protection agencies and focusing on consumer protection concerns.[24]<br><br>The Global Privacy Enforcement Network (GPEN) was formed in June 2007, when OECD governments adopted a Recommendation on Cross-border Cooperation in the Enforcement of Laws Protecting Privacy.[25] The Recommendation called for member countries to foster the establishment of an informal network of Privacy Enforcement Authorities.[26]<br><br>GPEN became on observer participant of ICPEN in 2017. This relationship allows GPEN to further its understanding of the importance, and increasing prevalence, of matters where privacy and consumer protection enforcement intersect.[27] Specifically, the GPEN's attendance at ICPEN as an observer allows each respective network to benefit from each other's relevant knowledge and enforcement experience.[28]<br><br>GPEN has also established the 'Network of Networks' project to connect GPEN with other international enforcement networks to share knowledge, experience and best practices. ICPEN is one of the networks to have joined the project. |
| European Union | - Policy | **Competition policy for the digital era[29]** |
| United Kingdom | - Policy | **Unlocking digital competition, Report of the Digital Competition Expert Panel[30]** |

[24] https://www.icpen.org/who-we-are
[25] https://www.privacyenforcement.net/
[26] https://www.privacyenforcement.net/
[27] https://icdppc.org/wp-content/uploads/2018/11/ICDPPC-DCCWG-Report-Final.pdf
[28] https://icdppc.org/wp-content/uploads/2018/11/ICDPPC-DCCWG-Report-Final.pdf
[29] http://ec.europa.eu/competition/publications/reports/kd0419345enn.pdf
[30] https://www.gov.uk/government/publications/unlocking-digital-competition-report-of-the-digital-competition-expert-panel

| Jurisdiction | Development type | Details |
|---|---|---|
| | | |
| European Consumer Consultative Group (ECCG) | - Policy | **Policy recommendations for a safe and secure use of artificial intelligence, automated decision-making, robotics and connected devices in a modern consumer world**[31] |
| European Commission | - Policy/legislation | **Targeted consultation on a draft Communication on the protection of confidential information for the private enforcement of EU competition law by national courts**[32] |

[31] https://ec.europa.eu/info/sites/info/files/eccg-recommendation-on-ai_may2018_en.pdf
[32] http://ec.europa.eu/competition/consultations/2019_private_enforcement/index_en.html

# Appendix H: Proposed Resolution

**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**

41st International Conference of Data Protection and Privacy Commissioners
21-24 Tirana, Albania

AUTHORS:

- The Office of the Privacy Commissioner of Canada (OPC) and the Office of the Australian Information Commissioner (OAIC) – on behalf of the *Digital Citizen and Consumer Working Group.*

CO-SPONSORS:

- *National Privacy Commission, Philippines*
- *Norwegian Data Protection Authority, Norway*
- *Information Commissioner's Office, United Kingdom*
- *European Data Protection Supervisor*
- *Federal Commissioner for Data Protection and Freedom of Information, Germany*
- *Belgian Data Protection Authority, Belgium*
- *Commission Nationale de l'Informatique et des Libertés, France*

NOTING that:

A. Statutory protections for individuals, whether as citizens or consumers, are imbedded in consumer protection, privacy and data protection laws;

B. The Conference's strategic priority to advance global privacy in the digital age by ensuring regulatory co-operation in achieving clear and consistently high standards of data protection, includes the strengthening of our connections and working with partners to achieve our mission of supporting authorities more effectively to include the protection of personal data in their mandates;

C. The Conference is committed to addressing the challenges related to privacy and data protection in the digital age;

D. Individuals are increasingly concerned about their lack of control over, and information about how, their information is processed and protected in the online environment;

E. Data protection authorities should cooperate with appropriate bodies that have an impact on, and can further the goal of protecting the rights of the individual in relation to their personal data;

F. Personal information is increasingly a core part of business models in the digital economy;

G. Privacy and data protection have become material considerations informing consumer decisions in the digital economy; and

H. Accordingly, there is a growing intersection of privacy, consumer protection, and competition issues.

RECALLING that:

I. The 39th and 40th Conferences resolved to identify the need for, and highlight ways to improve, collaboration between data protection and consumer protection authorities at both domestic and international levels with a view to fostering better protection for citizens and consumers in the digital economy.

HAVING made substantive progress by meeting the commitments of prior resolutions:

The 41st Conference resolves to renew and confirm the mandate of the DCCWG, for a period of two years, with a particular view to:

1. Continue to explore, understand and map the substantive overlaps between legislation regulating the data protection and/or privacy rights of individuals and legislation regulating competition or consumer protection laws, with a view to better understanding common policy themes identified by the DCCWG, and identifying further common policy themes.

2. Further sensitize authorities and networks to the intersections between privacy, consumer protection and competition such that competition and/or consumer protection authorities and data protection/privacy authorities can recognize the underlying principles which the different regulatory frameworks are subject to and can apply these principles into their regulatory activities to improve their enforcement practice.

3. Identify strategies, tools and collaboration vehicles that provide for cooperation across regulatory spheres, including actions which seek to:

    a. provide an avenue for competition/consumer authorities to seek answers on data protection/privacy issues, and vice versa.

   b. collaborate on common policy themes or topics.

4. Identify, recommend and/or advocate for such tools and instruments where they do not exist.

5. Support and facilitate collaborative initiatives across regulatory spheres.

6. Provide an update to the 42nd Conference on the working group's progress, and report back to the 43rd Conference on the elements listed above and if necessary, submit a resolution proposing specific measures or further concrete work.

# Appendix I: Forward Plan

**Digital Citizen and Consumer Working Group**

**2019-2020 Forward Looking Plan**

## 1) Background:

*The Digital Citizen and Consumer Working Group ("DCCWG") studies the intersections between privacy/data protection, consumer protection and competition. It was established via a resolution passed at the 39th International Conference of Data Protection and Privacy Commissioners ("ICDPPC" or "International Conference") and a second resolution was passed at the 40th International Conference which renewed and confirmed the mandate of the DCCWG to continue the study of these intersections.*

*The DCCWG is presenting a resolution at the 41st International Conference to renew and confirm the DCCWG's mandate for a further two years.*

## 2) Forward Plan for the Working Group 2019-2020

The DCCWG is proposing a resolution at the 41st International Conference which provides the key tasks to be undertaken by the DCCWG in the following two years (attachment A).

### Regulatory Co-operation

At the heart of the DCCWG's work is a recognition of the importance of regulatory co-operation in protecting personal information. Not only is this regulatory co-operation achieved between Data Protection and Privacy Authorities, but it also seeks to raise awareness and establish relationships between Data Protection and Privacy Authorities and Consumer Protection and/or Competition Protection Authorities.

The long term goal for the DCCWG includes advancing the will and realizing the mechanisms to collaborate with enforcement partners across regulatory spheres, with a view to having holistic and efficient regulatory outcomes that provide a greater

scope of coverage for consumers from privacy, consumer protection and competition risks.

The forward work plan of the DCCWG also seeks to achieve outcomes in both the Enforcement Co-operation and Policy Theme pillars identified in the 2019-2021 Strategic Plan of the International Conference.

**Policy Themes**

The DCCWG has, in its work over the past two years, identified certain areas of substantive overlap – for example:

i. Where the aims of Consumer Protection provisions may be closely aligned to those of Privacy and Data Protection:

   a. The requirement not to deceive, via false or misleading representations or material omissions; vs. the requirement for transparency or to obtain meaningful consent.

   b. The requirement not to use data in a way that would be unfair or harmful to consumers; vs. the requirement not to use information for illegitimate purposes and to properly safeguard information.

ii. Where Competition and Privacy / Data Protection laws have mutually relevant implications:

   a. Privacy implications resulting from mergers, or market concentration more generally.

   b. Competition implications resulting from privacy-law requirements, including where privacy may be a non-price element of competition.

Further work remains to be done by the DCCWG to better understand these, and other, common policy themes or substantive areas of mutual relevance to data protection and privacy authorities and consumer/competition authorities, with a view to providing opportunities and developing strategies further collaboration in those areas.[1]

This aim will be achieved by the continuation of mapping overlaps between data protection and Privacy authorities and consumer/competition authorities in different jurisdictions.[2] In particular, the DCCWG seeks to conduct and summarize legal research comparing privacy and data protection laws to those for competition and consumer protection, with a view to identifying potential overlaps and/or conflicts.[3]

[1] Refer to *ICDPPC 41st Conference, Proposed DCCWG Resolution,* paragraphs 3(b), 4, 5
[2] Refer to *ICDPPC 41st Conference, Proposed DCCWG Resolution,* paragraph 1
[3] Refer to *ICDPPC 41st Conference, Proposed DCCWG Resolution,* paragraph 1

## Enforcement Cooperation

The DCCWG workplan outlines opportunities for data protection authorities and consumer/competition authorities to develop the capacity to move forward in a co-ordinated approach to enforcement, to ensure that citizens of the global economy are kept safe.

The DCCWG is seeking to ensure that data protection authorities are aware of competition/consumer issues and vice versa. This work will require the continuation of DCCWG's current work to sensitize authorities and networks to the intersections between privacy, consumer protection and competition.[4]

The DCCWG will also seek to identify collaborative strategies, tools and vehicles that could support further cross-regulatory cooperation, with particular focus on those areas of substantive overlap outlined above.[5]

To these ends, the DCCWG will continue to engage, through meetings or workshops, with relevant networks, such as the Organisation for Economic Co-operation and Development ("OECD"), the Digital Clearinghouse ("DCH"), the Global Privacy Enforcement Network ("GPEN"), the International Consumer Protection Enforcement Network ("ICPEN"), the International Competition Network ("ICN") and the European Consumer Protection Cooperation Network ("CPC Network").

The DCCWG may also administer a common questionnaire to be answered by both data protection authorities and consumer/competition authorities on data protection issues and consumer/competition issues which may arise in both fields. Such questions may be around the definition of data controller/data processor in a multi-sided market, fairness and the use of consent, the impact of data protection authorities' actions/decisions on markets, definitions of harm, enforcement powers, and different rights and types of infringements under each regime.

It is envisaged that the DCCWG will recommend and advocate for collaboration tools and/or mechanisms where they do not exist, such as an avenue by which data protection authorities and consumer/competition authorities are able to share information, such as answers on issues within the other regulator's field.[6]

Finally, the DCCWG seeks to engage with our fellow ICDPPC members of the Working Group on International Enforcement Cooperation ("WGIEC") with a view to reflecting, in the Enforcement Cooperation Handbook, lessons learned regarding potential tools and strategies for cooperation where there is a cross-regulatory intersection.[7]

This will culminate in a recommended strategy for collaboration that will allow privacy and data protection authorities and consumer/competition authorities to more effectively achieve their respective aims.

---

[4] Refer to *ICDPPC 41st Conference, Proposed DCCWG Resolution, paragraph 2.*
[5] Refer to *ICDPPC 41st Conference, Proposed DCCWG Resolution, paragraph 3.*
[6] Refer to *ICDPPC 41st Conference, Proposed DCCWG Resolution,* paragraphs 3(a), 4, 5.
[7] Refer to *ICDPPC 41st Conference, Proposed DCCWG Resolution, paragraph 4.*

## Reporting

The DCCWG will provide an oral update and presentation on its workplan progress at the 42nd Conference, and a written report to the Conference at the 43rd Conference detailing the outcomes of its work over the previous two years (2019-2021), including lessons learned and any recommendations for further work in this area.

# ATTACHMENT A

**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**

41st International Conference of Data Protection and Privacy Commissioners

21-24 Tirana, Albania

AUTHORS:

- The Office of the Privacy Commissioner of Canada (OPC) and the Office of the Australian Information Commissioner (OAIC) – on behalf of the *Digital Citizen and Consumer Working Group.*

CO-SPONSORS:

- *National Privacy Commission, Philippines*
- *Norwegian Data Protection Authority, Norway*
- *Information Commissioner's Office, United Kingdom*
- *European Data Protection Supervisor*
- *Federal Commissioner for Data Protection and Freedom of Information, Germany*
- *Belgian Data Protection Authority, Belgium*
- *Commission Nationale de l'Informatique et des Libertés, France*

NOTING that:

A. Statutory protections for individuals, whether as citizens or consumers, are imbedded in consumer protection, privacy and data protection laws;

B. The Conference's strategic priority to advance global privacy in the digital age by ensuring regulatory co-operation in achieving clear and consistently high standards of data protection, includes the strengthening of our connections and working with partners to achieve our mission of supporting authorities more effectively to include the protection of personal data in their mandates;

C. The Conference is committed to addressing the challenges related to privacy and data protection in the digital age;

D. Individuals are increasingly concerned about their lack of control over, and information about how, their information is processed and protected in the online environment;

E. Data protection authorities should cooperate with appropriate bodies that have an impact on, and can further the goal of protecting the rights of the individual in relation to their personal data;

F. Personal information is increasingly a core part of business models in the digital economy;

G. Privacy and data protection have become material considerations informing consumer decisions in the digital economy; and

H. Accordingly, there is a growing intersection of privacy, consumer protection, and competition issues.

RECALLING that:

I. The 39th and 40th Conferences resolved to identify the need for, and highlight ways to improve, collaboration between data protection and consumer protection authorities at both domestic and international levels with a view to fostering better protection for citizens and consumers in the digital economy.

HAVING made substantive progress by meeting the commitments of prior resolutions:

The 41st Conference resolves to renew and confirm the mandate of the DCCWG, for a period of two years, with a particular view to:

1. Continue to explore, understand and map the substantive overlaps between legislation regulating the data protection and/or privacy rights of individuals and legislation regulating competition or consumer protection laws, with a view to better understanding common policy themes identified by the DCCWG, and identifying further common policy themes.

2. Further sensitize authorities and networks to the intersections between privacy, consumer protection and competition such that competition and/or consumer protection authorities and data protection/privacy authorities can recognize the underlying principles which the different regulatory frameworks are subject to and can apply these principles into their regulatory activities to improve their enforcement practice.

3. Identify strategies, tools and collaboration vehicles that provide for cooperation across regulatory spheres, including actions which seek to:

    a. provide an avenue for competition/consumer authorities to seek answers on data protection/privacy issues, and vice versa.

    b. collaborate on common policy themes or topics.

4. Identify, recommend and/or advocate for such tools and instruments where they do not exist.

5. Support and facilitate collaborative initiatives across regulatory spheres.

6. Provide an update to the 42nd Conference on the working group's progress, and report back to the 43rd Conference on the elements listed above and if necessary, submit a resolution proposing specific measures or further concrete work.