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

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.