THE CANADIAN BAR REVIEW

LA REVUE DU BARREAU CANADIEN

Vol. 102 2024 No. 1

ALGORITHMIC PERSONALIZED PRICING: A PERSONAL DATA PROTECTION AND CONSUMER LAW PERSPECTIVE

Pascale Chapdelaine[1]

Price is often the single most important term in consumer transactions. As the personalization of e-commerce continues to intensify, the law and policy implications of algorithmic personalized pricing i.e., to set prices based on consumers' personal data with the objective of getting as closely as possible to their maximum willingness to pay (APP), should be top of mind for regulators. This article looks at the legality of APP from a personal data protection law perspective, by first presenting the general legal framework applicable to this commercial practice under competition and consumer law. There is value in analysing the legality of APP through how these bodies of law interact with one and the other. This article questions the legality of APP under personal data protection law, by its inability to effectively meet the substantive requirements of valid consent and reasonable purpose. Findings of illegality of APP under personal data protection law may in turn further inform the lawfulness of APP under competition and consumer law.

Le prix est souvent le plus important facteur dans les transactions des consommateurs. Alors que la personnalisation du commerce électronique continue de s'intensifier, les implications juridiques et politiques de la tarification personnalisée algorithmique, c.-à-d. fixer les prix en fonction

[1] Pascale Chapdelaine is an Associate Professor at the University of Windsor, Faculty of Law. Thanks to the University of Windsor, Faculty of Law for research grants making this publication possible, and for the excellent research assistance of Windsor Law students at various stages of the research between 2020–2023: Samuel Abbott, Lauren Tsogaz, Rushi Chakrabarti, Abhishek Chaudhry, Marc Begin, and Summer Samra. I also thank the two anonymous peer reviewers for their very insightful comments, and the editors of the Canadian Bar Review/ La Revue du Barreau Canadien.

des données personnelles des consommateurs dans le but de se rapprocher autant que possible de leur volonté maximale de payer, devraient être au centre des préoccupations des organismes de réglementation. L'auteure de cet article examine la légalité de la tarification personnalisée algorithmique dans une perspective de protection des données personnelles, en présentant d'abord le cadre juridique général applicable à cette pratique commerciale en vertu du droit sur la concurrence et de la consommation. Il est probant d'analyser la légalité de cette méthode de tarification à travers la manière dont ces lois interagissent. L'auteure remet en cause la légalité de la tarification personnalisée algorithmique en vertu de lois sur la protection des renseignements personnels, en raison de son incapacité à répondre efficacement aux exigences substantielles de la validité du consentement des motifs raisonnables. Les constatations d'illégalité de cette méthode de tarification en vertu de ces lois peuvent à leur tour éclairer davantage sa légalité en vertu du droit sur la concurrence et de la consommation.

Contents

1. Introduction

As the personalization of e-commerce transactions continues to intensify, the law and policy implications of algorithmic personalized pricing should be top of mind for regulators. Price is often the single most important term of consumer transactions. Algorithmic personalized pricing (APP) is a form of online discriminatory pricing practice whereby suppliers set prices based on consumers' personal information with the objective of getting as closely as possible to their maximum willingness to pay.[2] As such, APP raises issues of competition, contract, consumer protection, privacy, personal data protection, and anti-discrimination law.

This article looks at the legality of APP from a Canadian perspective under personal data protection law, by first presenting the general legal framework applicable to this commercial practice under competition and consumer law. While compliance with anti-discrimination law is often raised regarding the legality of APP,[3] it is beyond the scope of this article to examine this body of law.[4] To our knowledge, there is no Canadian statute or court decision specifically addressing the legality of APP. As such, there is added value to assess the legality of APP through the various bodies of law studied in this article and how they interrelate with one another. The analysis of personal data protection law conducted here may shed new light on the legality of APP under consumer law and further expose competition law shortcomings to adequately deal with the effects of firms' extraction of big data in the digital marketplace.

2. Algorithmic Personalized Pricing

Algorithmic personalized pricing (or APP), refers to the commercial practice by which firms set prices according to a consumer's personal characteristics, targeting as closely as possible their maximum willingness

---

2 See section 2 "Algorithmic Personalized Pricing" below.

3 See e.g. Ariel Ezrachi & Maurice Stucke, *Virtual Competition: The Promise and Perils of the Algorithm-Driven Economy* (Cambridge: Harvard University Press, 2016) at 124–127; Organisation for Economic Co-operation and Development, "Personalized Pricing In The Digital Era—Note By The European Union" (23 November 2018) at 40–41, online (pdf): <https://tinyurl.com/tz5m7dxb> [perma.cc/8GD2-QTXX] [OECD EU Submission]; Alan M. Sears, "The Limits of Online Price Discrimination in Europe" (2019) 21 Colum Sci & Tech L Rev 1 at 27–36. See also *infra* note 162 (on discrimination in contravention of human rights laws not meeting the reasonable purpose requirement under personal data protection law).

4 In Canada, the applicable body of law comprises federal and provincial human right codes applicable to the private sector. The legality of APP under anti-discrimination law is the object of a separate research project and forthcoming article by this author.

to pay (or *reservation price*).[5] Often referred to as "perfect price discrimination", it contrasts with *versioning* (offering different prices for different versions of a good or service)[6] or *group pricing* (charging different prices to different groups of consumers based on a personal characteristic they share, e.g., age, gender, or student status).[7] APP should not be confused with *dynamic pricing*, where prices vary based on offer and demand rather than by discriminating on an individual's personal characteristics.[8] However, in practice, given the opacity of pricing techniques and limited ability to distinguish between APP and dynamic pricing, the line between the two may be blurry at times.[9] APP is different from *price steering* or *targeted advertising*. For those commercial practices, firms will use consumer personal characteristics. In that sense, firms exercise some discrimination, however not on the price *per se*, but in the order with which they list offers for goods or services, or in the selection of advertising displayed to the consumer.[10]

While earlier economic studies have been guarded on the extent to which APP occurs, for lack of substantiated empirical research, and based on traditional economic theory requirements for APP (or first-degree price discrimination) to occur, there is growing evidence that firms are resorting to APP in online transactions.[11] APP is also likely to occur in

---

5 Organisation for Economic Co-operation and Development, "Personalized Pricing In The Digital Era" (28 November 2018) at 9, online (pdf): <https://tinyurl.com/yc2jjfzv> [perma.cc/9FFR-EXUQ] [OECD Competition Committee]; Ezrachi & Stucke, *supra* note 3 at 85–86.

6 OECD Competition Committee, *supra* note 5 at 9; Akiva Miller, "What Do We Worry About When We Worry About Price Discrimination? The Law and Ethics of Using Personal Information for Pricing" (2014) 19 J of Tech L & Pol'y 41 at 55; Christopher Townley, Eric Morrison & Karen Yeung, "Big Data and Personalized Price Discrimination in EU Competition Law" (2017) at 6, online (pdf): <https://tinyurl.com/ypyw7hrz> [perma.cc/YA4D-W9EU].

7 OECD Competition Committee, *supra* note 5 at 9. See also Miller, *supra* note 6 at 55; Townley, Morrison & Yeung, *supra* note 6 at 7.

8 OECD Competition Committee, *supra* note 5 at 9; Ezrachi & Stucke, *supra* note 3 at 87–88.

9 Ezrachi & Stucke, *supra* note 3 at 87–88.

10 OECD Competition Committee, *supra* note 5 at 9–10; see also Ezrachi & Stucke, *supra* note 3 at 107–08.

11 Pascale Chapdelaine, "Algorithmic Personalized Pricing" (2020) 17:1 NYU J of L & Bus 1 at 12–14 (citing several studies on the existence of APP as widespread commercial practice). See also Ethan Wilk, "An Old-Fashioned Economic Tool Can Tame Pricing Algorithms—Left Unchecked, Pricing Algorithms Might Unintentionally Discriminate and Collude to Fix Prices" (26 April 2022), online: <https://tinyurl.com/mswwfyu6> [perma.cc/9WBT-BCU2].

payment-less brick-and-mortar stores.[12] The traditional economics theory preconditions for APP to occur, i.e., (i) the ability to assess consumers' individual willingness to pay, (ii) the absence of or limited arbitrage,[13] and (iii) presence of market power,[14] need to be reconsidered in the online e-commerce environment. Suppliers' increasingly powerful tools and use of personal data influence online consumer purchasing decisions. This may lead to "micro-marketplace chambers", where consumers' judgements of competitive alternatives in the marketplace are blurred.[15] This phenomenon is amplified for customers of large retail or service platforms (e.g., Amazon, Uber) where market power and control may hide beneath seemingly competitive prices.[16] To be sure, APP may occur even for goods or services susceptible to arbitrage (i.e., which can be resold), or in (imperfectly) competitive markets.[17]

Various surveys indicate a strong consumer dislike of discriminatory pricing, viewing it as unfair.[18] As a result of consumers' disapproval of

---

[12] "Amazon Go" brick and mortar retail stores are highly personalized payless stores. See Andria Cheng, "Why Amazon Go May Soon Change The Way We Shop" (13 January 2019), online: <https://tinyurl.com/3rfj6j8r> [perma.cc/UVY8-W2HD].

[13] I.e., the limited ability of buyers to resell goods or services acquired from suppliers, such as non-transferable purchases (airline tickets, hotel bookings), which would create a market that competes with the suppliers' market.

[14] Ezrachi & Stucke, *supra* note 3 at 86–87; OECD Competition Committee, *supra* note 5 at 13; Gerhard Wagner & Horst Eidenmüller, "Down by Algorithms? Siphoning Rents, Exploiting Biases, and Shaping Preferences: Regulating the Dark Side of Personalized Transactions" (2019) 86:2 U Chicago L Rev 581 at 585–86; Oren Bar-Gill, "Algorithmic Price Discrimination When Demand is a Function of Both Preferences and (Mis)perceptions" (2019) 86 U Chicago L Rev 217 at 227. To these traditional pre-conditions, one may add the ability to conceal the practice of personalized pricing to buyers: Chapdelaine, *supra* note 11 at 17–18.

[15] See Ezrachi & Stucke, *supra* note 3 at 108–09. I make reference here to "micro-market-place chambers", by analogy to the phenomenon of "echo chambers".

[16] Ezrachi & Stucke, *supra* note 3 at 208–11 (on the lack of transparency in Uber algorithmic surge price settings and market power leading to the illusion of a competitive price).

[17] Miller, *supra* note 6 at 54, 57; Andrew Odlyzko et al, "Privacy, Economics, and Price Discrimination on the Internet" in *2003 IEEE International Conference on Electronic Commerce* (California: IEEE Computer Society, 2003) at 358 (describing the recognition within economic literature that price discrimination can arise in a competitive environment).

[18] See Option Consommateurs, "Changes to Prices Advertised online: Analysis of Business Practices and the Legal Framework in Canada" (June 2018) at 34–36, online (pdf): <https://tinyurl.com/ynd5x4cs> [perma.cc/352J-8CHA]; Joseph Turrow, Lauren Feldman & Kimberly Meltzer, "Open to Exploitation: America's Shoppers Online and Offline" (1 June 2005), online: <https://tinyurl.com/4xcbcn5t> [perma.cc/JG9L-TBGB]; OECD Competition Committee, *supra* note 5 at 24–5; European Commission, "Consumer Market Study on Online Market Segmentation Through Personalized Pricing/

discriminatory pricing, one can reasonably predict that retailers will either refrain from the practice or conceal it. In fact, the ability to conceal APP is arguably another pre-condition to APP effectively taking place, and one that demands greater regulatory scrutiny.[19] The lack of transparency surrounding APP raises issues on the scope of suppliers' obligations to disclose information that is material to a transaction in commercial law, as well as to the requirement of meaningful consent in personal data protection law.[20]

Offers in the European Union" (2018), online (pdf): <https://tinyurl.com/24ksvyjx> [perma.cc/3K7R-Y3XX]; Citizens Advice, "A Price of One's Own An Investigation into Personalized Pricing in Essential Markets" (31 August 2018) at 1, online: <https://tinyurl.com/4evm3h9e> [perma.cc/C65R-6J8M]; Joost Poort & Frederik J. Zuiderveen Borgesius, "Does everyone have a price? Understanding people's attitude towards online and offline price discrimination" (2019) 8:1 Internet Pol'y Rev 1 (analysis of two surveys conducted in the Netherlands, whereby the vast majority of consumers viewed the practice of online price discrimination as unfair); Victor Vijay, Maria Fekete Farkas & Zoltán Lakner, "Consumer Attitude and Reaction Towards Personalized Pricing in the E-Commerce Sector" (2019) 4:2 J of Management & Marketing Rev 140; Anna Priester, Thomas Robbert & Stefan Roth, "A Special Price Just for You: Effects of Personalized Dynamic Pricing on Consumer Fairness Perceptions" (2020) 19 J of Revenue and Pricing Management 99; Willem H. van Boom et al, "Consumers Beware: Online Personalized Pricing in Action! How the Framing of a Mandated Discriminatory Pricing Disclosure Influences Intention to Purchase" (2020) 33 Social Justice Research 331; Gabriele Pizzi et al, "Privacy concerns and justice perceptions with the disclosure of biometric versus behavioral data for personalized pricing: Tell me who you are, I'll tell you how much you pay. Consumers' fairness and privacy perceptions with personalized pricing" (2022) 148 J of Bus Research 420; on the practice of personalization more generally, see also Department for Business, Energy & Industrial Strategy, "Modernising consumer markets: Consumer Green Paper" (April 2018) at para 124, online (pdf): <https://tinyurl.com/yf4a96cv> [perma.cc/HJZ3-J9CJ] (finding that 78% of UK internet users "perceive personalisation to be unfair" and "that online platforms should be regulated to limit the extent" of personalization).

19 Chapdelaine, *supra* note 11 at 17–18.

20 Frank Pasquale, *The Black Box Society: The Secret Algorithms That Control Money And Information* (Cambridge: Harvard University Press, 2016) at 3 ("The law, so aggressively protective of secrecy in the world of commerce, is increasingly silent when it comes to the privacy of persons"); Soshana Zuboff, *The Age Of Surveillance Capitalism* (New York: Public Affairs, 2019) at 338–45 (listing several factors explaining how "surveillance capitalists" have been able to get away for so long with concealing personal data handling practices from their consumers and the public; among them, consumers' self-interest, social persuasion, inevitabilism, ignorance, and unprecedented, i.e. *sui generis* environment, logic and methods that were initially impossible to comprehend).

3. The Regulation of Pricing Terms in Competition Law and in Consumer Law

A) Overview

There is a presumption in liberal free-market democracies that firms are generally free to set the prices at which they sell their products.[21] This assumption rests on the free exercise of parties' choice and autonomy leading them to buy and sell products at an agreed price or *fair market value*. In mass-consumer markets, the precept is that competition has self-regulatory effects that keep prices close to marginal costs, for the ultimate benefit of consumers. Save for specific price gouging prohibitions in consumer transactions, or more general common law doctrines protecting weaker parties, whereby pricing terms are subject to greater scrutiny, the endorsement of pricing freedom rejects "just price" theories, or the notion of inherently fair prices.[22]

Economic sectors involving (quasi) monopolistic or low-competition markets (e.g., utilities, telecommunications, patented medicines), or industries at a higher risk of exploiting consumers' vulnerability have regulations affecting pricing terms.[23] Credit and financial services are heavily regulated at the federal and provincial levels given the vulnerability that surrounds credit, borrowing, financial investments, and the high political stakes to prevent any potentially abusive commercial practices.[24] Industry-specific legislation impacting pricing terms also target areas of the economy where consumers are more likely to be vulnerable given high-pressure sale environments.[25]

Competition law, general common law, civil law contract law doctrines, and consumer protection statutes affect pricing terms at their periphery, e.g., by requiring disclosure of essential contract terms, or by constraining various forms of misrepresentations about the actual price (e.g., drip pricing, false sales etc.). At the macro-economic level, regulation geared towards facilitating competitive markets directly targets pricing

---

21 Miller, *supra* note 6 at 68, 75–76.

22 *Ibid*.

23 See Joshua Karton, "Piecemeal Solutions to Demonstrated Problems of Unfairness: Control of Price Terms in Common Law Canada" in *Control of Price Related Terms in Standard Form Contracts,* ed by Yesim M. Atamer & Pascal Pichonnaz (Basel: Springer International Publishing, 2019) at 10–16 (discussing Canadian industry-specific regulation affecting pricing terms at the federal and provincial levels).

24 *Ibid* at 11–13.

25 Those include consumer protection statutes regulation of door-to-door selling, funeral services, personal development services, and automotive vehicle repairs.

practices that have anti-competitive effects (collusion, price fixing, abuse of a dominant position, etc.).

The following sections provide an overview of how competition law and consumer law regulate pricing terms and how those bodies of law apply to APP.

B) Competition Law

The *Competition Act*[26] regulates various anti-competitive practices through criminal and civil sanctions. The Act has largely remained unchanged since 1986, except for relatively minor amendments, including in 2009, and more recently in 2022 and 2023.[27] The underlying purpose of the Act is to promote overall economic welfare, which translates into the following objectives: (i) the efficiency and adaptability of the Canadian economy, (ii) expanding opportunities for Canadian participation in world markets, while recognizing the role of foreign competition in Canada, (iii) ensuring equitable opportunity for small and medium-sized enterprises to participate in the Canadian economy, and (iv) to provide consumers with competitive prices and product choices.[28] Such statutory objectives are geared to the market at the macro level, and on interactions between competitors, leaving consumer rights and interests as one factor to be balanced against many others.

This section provides a brief overview of the *Competition Act's* macro-market regulation of anti-competitive practices and its application to APP. It also applies the Act's deceptive marketing practice provisions to APP. Third, it points to the impetus to rethink competition law and policy in light of the digital marketplace, privacy, and big data.

1) Macro-market Anti-competitive Practices

The regulation of macro-market anti-competitive practices has been covered extensively in recent scholarly work and policy reports on discriminatory pricing, algorithms, and big data.[29] "Macro-market anti-

---

26 *Compeition Act*, RSC 1985, c C-34.

27 *Budget Implementation Act, 2022, No. 1,* SC 2022, c 10; *Affordable Housing and Groceries Act*, SC 2023, c 31. The *Competition Act* is currently undergoing a major legislative review: see discussion below in this section. For a brief history of competition law and the main evolutive trends of Canadian competition policy, see Michael Trebilcock & Francesco Ducci, "*The Evolution of Canadian Competition Policy: A Retrospective*" (2018) 60:2 Can Bus LJ 171.

28 *Competition Act*, *supra* note 26, s 1.1.

29 See generally Ezrachi & Stucke, *supra* note 3; Townley et al, *supra* note 6; Inge Graef, "Algorithms and Fairness: What Role for Competition Law in Targeting Price

competitive practices" refers to conduct primarily involving business-to-business competitors in a given market segment, as opposed to practices involving more direct supplier and buyer relationships.[30] This section looks at the interface between APP and the macro-market aspects of competition law, and the conclusions to derive therefrom.

At the macro-market regulation level, aside from instances where the practice of APP is connected to collusion, cartels,[31] amounts to abuse of a dominant position[32] including predatory pricing,[33] or consists of price maintenance,[34] or delivered pricing,[35] there is no consensus on the effects of APP on competition (positive or negative).[36] Unlike other jurisdictions such as the US, there is no provision in the *Competition Act* specifically prohibiting discriminatory pricing.[37] A generally accepted

---

Discrimination Towards End Consumers?" (2017) 24:3 Colum J Eur L 541; Miller, *supra* note 6 at 65–66, 70–74; OECD Competition Committee, *supra* note 5 at 26–32.

30 E.g. misleading advertising practices which we discuss further below in this section.

31 *Competition Act*, *supra* note 26, s 45. See Plea Agreement, *United States v David Topkins* (30 April 2015), online (pdf): <https://tinyurl.com/3tenspjb> [perma.cc/8TZP-V9HK]; Information, *United States v David Topkins*, (6 April 2015), online (pdf): <https://tinyurl.com/34p73mms> [perma.cc/7X6E-JSMU] (US Department of Justice prosecution against illegal price-fixing cartel that shared dynamic pricing algorithms for sale of posters on the Amazon Market place); see also Terrell McSweeny & Brian O'Dea, "The Implications of Algorithmic Pricing for Coordinated Effects Analysis and Price Discrimination Markets in Anti-Trust Enforcement" (2017), online (pdf): <https://tinyurl.com/2aakje4v> [perma.cc/TD3S-S8LH]; see also Emilio Calvano et al, "Artificial Intelligence, Algorithmic Pricing, and Collusion" (2020) 110:10 American Economic Rev 3267 (AI simulated models research suggesting that autonomous pricing algorithms may lead to collusion overtime between competing firms even if not specifically instructed to do so).

32 *Competition Act*, *supra* note 26, s 79.

33 *Ibid*, ss 78(1)(i), 79.

34 *Ibid*, s 76 (regarding suggested retail or resale prices as potential anti-competitive practices).

35 *Ibid*, ss 80–81 (i.e. "... refusing a customer … delivery of an article at any place in which the supplier engages in a practice of making delivery of the article to any other of the supplier's customers" only because the first-named customer business is in another location (and even if that customer agrees to take on delivery at the usual delivery location of the supplier)).

36 Chapdelaine, *supra* note 11 at 26–29 (providing a brief survey of literature about the effects of discriminatory pricing on competition).

37 *Robinson-Patman Act of 1936,* 15 USC § 13(a)–(f), pursuant to which it is illegal to discriminate on price between different purchasers of like grade and quality where the effect is to substantially lessen competition, unless different treatment is based on a specific legal base. This provision has rarely been enforced and is criticized for its convolutedness and efficacy in addressing anti-competitive behaviour: see e.g. Miller, *supra* note 6 at 71–72. Canada had a similar prohibition in the *Competition Act*, s 50 which was repealed in amendments in 2009 to the *Competition Act*, *supra* note 26.

view is that APP is not unlawful per se except in the above mentioned cases.[38] Academic and policy reports tend to focus on abuse of a dominant position as a main area of concern for APP.[39] This necessarily narrows the analysis to larger suppliers conducting business online, while large segments of e-commerce suppliers involve small to medium suppliers.[40] The greater attention to abuse of a dominant position provisions is based on the assumption that APP is more likely to be used by firms enjoying significant market power.[41] To the extent that APP may occur in (imperfectly) competitive markets as well, this leaves a huge gap that the current regulation of macro-market anti-competitive practices does not address.[42] Furthermore, such macro-market regulation operates at the business competitors' level, more remote from supplier-consumer practices by not questioning personalized pricing at the substantive level (e.g., issues of fairness, privacy, deception, and discrimination).

The determination of the (anti)competitive effects of APP depends in large part on the goals pursued behind competition law and policy. If the goal is to increase overall consumer welfare, then APP, which is more likely to decrease consumer welfare by reducing consumers' surplus, even in (imperfectly) competitive markets, might deserve closer scrutiny as a potentially anti-competitive practice.[43] On the other hand, if the objective of competition law and policy as it is arguably the case in Canada,[44] is

---

38 See e.g. Townley et al, *supra* note 6 at 50 & fol. (based on an extensive analysis from an EU competition law perspective).

39 See OECD Competition Committee, *supra* note 5 at 26–32 (focusing competition law analysis of instances where discriminatory pricing may be illegal when the practice amounts to abuse of a dominant position).

40 *Ibid* at 30 at para 74.

41 *Ibid* at 26–32. See *supra* section 2 "Algorithmic Personalized Pricing" (about conditions required for personalized pricing to occur).

42 See Rebecca Kelly Slaughter, Janice Kopec, & Mohamad Batal, "Algorithms and Economic Justice: A Taxonomy of Harms and a Path Forward for the Federal Trade Commission" (2021) 23 Yale J of L & Tech 1 at 34–35 (on the fact that "even absent collusion, algorithms can fuel personalized pricing practices that may alter the competitive dynamics of a market in ways that harm consumers" including, but not exclusively through price increases).

43 Including beyond abuse of a dominant position, collusion, cartel, predatory pricing and other anti-competitive practices. See Douglas M. Kochelek, "Data Mining and Antitrust" (2009) 22:2 Harv JL & Tech 515 at 535 (arguing that "[d]ata-mining-based price discrimination schemes fall into a gap between antitrust doctrine and the policies underlying the doctrine", comparing business practices seeking to assess a consumer maximum willingness to pay have similar anti-competitive effects as price fixing practices); for a critique of Kochelek position as failing to consider other potential positive competitive effects of APP, see Miller, *supra* note 5 at 72–74.

44 *Competition Act*, *supra* note 26, s 1.1 lists its objectives as promoting and balancing various (at times competing) interests.

to increase overall economic or social welfare, then any consumer harm resulting from APP could be offset by increased firms' revenues, with more or less neutral effects on overall social or economic welfare.[45] Regardless of the overarching competition law and policy goals, so-called overall positive competition law effects should never be made on the back of deceptive or detrimental practices for consumers.[46]

2) Deceptive Marketing Practices

The *Competition Act*'s regulation of misleading advertising, including the recent tightening of rules applicable to false discount advertisements are only tangentially relevant to APP. Generally, a person who "makes a representation to the public that is false or misleading in a material respect" engages in reviewable conduct under the *Competition Act*.[47] The commercial practice of APP does not lead to a misleading representation as such, to the extent that the price is clearly advertised to the consumer (and remains unchanged up to payment stage) and that there are no representations to the effect that all consumers are charged the same price for a similar product.

Various forms of deceptive marketing practices pertain to how price is displayed to consumers. The explicit regulation of *drip pricing*, whereby additional mandatory fees increase the final price paid from the price initially advertised was recently added to the *Competition Act*.[48] It specifically targets online e-commerce transactions where adding fees upon payment to initially advertised price is common.[49] Drip pricing is a variant of the general provision ensuring consistency in pricing from

---

45 Herbert Hovenkamp, "Antitrust in 2018: The Meaning of Consumer Welfare Now" (2018) 6:8 Penn Wharton Pub Pol'y Initiative 1 at 3 (pointing out that general welfare test balances consumer harm against producer benefits and that its application can lead to accepting a significant amount of market power as not being anti-competitive).

46 Robert M. Weiss & Ajay K. Mehrotra, "Online Dynamic Pricing: Efficiency, Equity and the Future of e-Commerce" (2001) 6 Va JL & Tech 11 ("… price discrimination may perhaps promote an efficient use of a society's resources. In many cases, however, efficiency must be balanced against the need to achieve equitable treatment of individual consumers" at para 3).

47 *Competition Act*, *supra* note 26, s 74.01(1)(a). The federal regulation of deceptive marketing practices may overlap with provincial powers to regulate contracts and torts as discussed below in this section. The disruption of competitive processes through misinformation, and its impact on the integrity of the marketplace are invoked to justify federal powers over deceptive marketing practices: see ISED, Future of Competition Policy, *infra* note 59 at 48.

48 *Ibid*, s 74.01(1.1), s 52(1.3) added to the *Competition Act* in June 2022.

49 Competition Bureau of Canada, "The Competition Bureau of Canada participates in consultation to modernize Canadian competition policy" (8 February 2022), online: <https://tinyurl.com/yfsnfzt8> [perma.cc/X2VV-HLB6].

advertisement to point of sale, by prohibiting sales above the advertised price.[50] These prohibitions affect APP only to the extent that the personalization involves mandatory extra fees in addition to the price initially advertised.

Other regulated deceptive practices deal with statements presenting price in a false light to make it more attractive through misleading surrounding context. "On Sale" in reference to "ordinary" or "regular price", "bargains", and "bait and switch"[51] selling statements are reviewable practices under the *Competition Act*.[52] The Act requires that a supplier making statements about "savings" prove the validity of the ordinary selling price by satisfying either a sales "volume test"[53] or a "time test"[54] regarding prior sales (or offers for sale) at the "ordinary" or "regular price". In effect, the product must have either been sold at the regular price at a substantial volume for a reasonable period of time, or it must have been offered at the regular price in good faith for a substantial period of time.

---

50 *Competition Act*, *supra* note 26, ss 74.05(1),(3) which target advertisements with respect to parties that it "could reasonably be expected to reach" unless "narrowed by reference to a geographical area, store, department of a store, sale by catalogue or otherwise".

51 *Competition Act*, *supra* note 26, s 74.04(1) (bargain pricing & bait and switch selling refers to situations where the supplier that sells at a 'bargain' does not have sufficient quantities in the context of their business to lawfully engage in that kind of advertisement).

52 *Competition Act*, *supra* note 26, ss 74.01(2)–(5).

53 *Ibid*, ss 74.01(2)(a),(3)(a) (a "substantial volume" of the product must have been sold at the regular price within a reasonable period of time before or after the making of the representation; Competition Bureau of Canada, "Ordinary Price Claims–Enforcement Guidelines" (16 October 2009) s 4.2.1, online: <https://tinyurl.com/44y39yw6> [perma.cc/JZ82-35N2] (The Competition Bureau considers more than 50% of sales at (or above) the regular price to constitute a "substantial volume", for the purposes of the volume test, and 12 months before or after the claim to be a "reasonable period of time" (which could be shorter or longer depending on the nature of the product)).

54 *Competition Act*, *supra* note 26, ss 74.01(2)(b),(3)(b); Ordinary Price Claims–Enforcement Guidelines, *supra* note 53, s 4.2.2 (the product must have been offered at the regular price in good faith for a substantial period of time recently before or immediately after the making of the representation. A "substantial period of time" means more than 50% of the 6 months before or after the claim was made, depending on the nature of the product. Whether the product has been sold in good faith depends on a list of non-exhaustive factors: *Ibid*, s 4.2.2.1: whether "(i) the product was openly available in appropriate volumes; (ii) the reference price was based on sound pricing principles and/or was reasonable in light of competition in the relevant market during the time period in question; (iii) the reference price was a price that the supplier fully expected the market to validate, whether or not the market did validate this price; and/or (iv) the reference price was a price at which genuine sales had occurred, or it was a price comparable to that offered by competitors).

These provisions regulating "on sale" or similar references to a regular price apply whether the supplier refers to its own price or the market price.[55] It is unclear how a supplier resorting to APP would be able to comply with the "ordinary price" measurement when advertising a sale or bargain relative to this suppliers' regular price. If prices are constantly adapted algorithmically and individually to each potential consumer's data profile, what is the "ordinary price" of any given product to which the sale price refers to? And if the supplier meets the sales volume threshold at the "ordinary price" (which allows some price fluctuations by including higher sales prices than the stated "ordinary price") can we state that this "ordinary price" has been publicly made available, given all the possible variations? As major legislative reform is underway, it is hoped that Canada will be more attuned to these questions and other significant changes brought on to the commercial transactions landscape by the digital marketplace and extraction of big data. There is a growing awareness of the need for a major reset of how we approach competition law and policy.

3) Assessment: Competition Law, Big Data, and the Digital Marketplace

Initially, government agencies including Canada's Competition Bureau, viewed digital platforms and big data commercial practices, e.g., personalized advertising favourably, steering innovation, competition, and benefiting consumers.[56] There is now a growing recognition that firms' control and use of consumers' and other data can significantly increase market power and lead to abuse, as well as create barriers to entry for smaller competitors.[57] The US Federal Trade Commission recently launched an investigation into *commercial surveillance* business practices through massive collection of personal data and consumer

---

[55] *Competition Act*, *supra* note 26, ss 74.01(2)–(3) (referring respectively to regular market price in a relevant geographical area and to a representation made by the supplier).

[56] Competition Bureau of Canada, "Big Data and Innovation: Key Themes for Competition Policy in Canada" (19 February 2018) at 5, online: <https://tinyurl.com/24warhzn> [perma.cc/RPB3-AEAX] ("Competition law and policy should continue to rely on market forces to lead to beneficial outcomes, not regulate prices or other outcomes").

[57] Lina M. Khan, "Amazon Antitrust Paradox" (2017) 126:3 Yale LJ 710 at 743; see also Anca Chirita, "Abuse of Global Platform Dominance or Competition on the Merits?" (2021) 33:1 Loy Consumer L Rev 1 (arguing that the handling of personal data by global platforms is not only a matter of data privacy law but also a matter of competition law that merits an investigation into "how digital dominance has been strengthened through the downfall of emerging competition (the exclusionary harm) and the excessive combination of individuals' data (exploitative harm)" at 1).

profiling.[58] Canada's current competition law legislative reform objectives have a similar focus on big data and the digital marketplace, and include alignment with the direction of its major trading partners.[59]

The Canadian Ministry of Innovation, Science and Economic Development recently published a report inviting comments for competition legislative reform, targeting large online platforms and big data.[60] Notably, the report does not specifically mention APP or other forms of personalization as areas of further study.[61] The report raises concerns around the dangers of increased collusion favoured by the opacity of algorithms,[62] the non-price competition features of the digital marketplace, such as network effects, and the competitive advantage of digital platforms through their large customer base personal data pools.[63] These customer data pools are a commodity in themselves: they become a parallel source of revenue through their sale to data brokers, are utilised in advertising, to sell, to give away products, and create additional barriers to entry for smaller competitors.[64] The report also refers to the practice of "self preferencing", such as when e-commerce platforms create a marketplace for suppliers, while also selling their own products, taking advantage of the control they have over their platform by favouring their products over those of the competing suppliers.[65] The report raises concerns about the concentration of power that resides in very few gatekeepers (i.e., Google for online search, Facebook (Meta) for social media, and Amazon for

---

58 Federal Trade Commission, "Commercial Surveillance and Data Security Rulemaking" (11 August 2022), online: <https://tinyurl.com/45hnn6kk> [perma.cc/MZU6-6DD9]. See also Slaughter et al, *supra* note 42 (on how various tools available to the US Federal Trade Commission could be used more pro-actively to address the detrimental effects of the digital marketplace on competition and consumers; pointing to pricing algorithms as a potential area of concern which may lead to overall price increases by targeting as closely as possible to consumers' maximum willingness to pay: *Ibid* at 34–35).

59 Innovation, Science and Economic Development Canada, "The Future of Competition Policy in Canada" (18 November 2022), online (pdf): <https://tinyurl.com/3ujzemtm> [perma.cc/3D9V-P6VD] (the Government of Canada "is committed to a renewed role for the Competition Bureau in protecting the public in our modern marketplace, in line with steps taken by many of Canada's key international partners" at 4) [ISED, Future of Competition Policy].

60 *Ibid*. Upon finalization of this article, Bill C-59, *Fall Economic Statement Implementation Act, 2023*, 1st Sess, 44th Parl, was introduced (first reading 30 November 2023) which if enacted will bring several changes to the *Competition Act, supra* note 26.

61 See Ezrachi & Stucke, *supra* note 3 at 219–24 (on key challenges to competition enforcement in digital markets, including a difficulty to identify anti-competitive issues, or lack of tools to fix the identified problems).

62 ISED, Future of Competition Policy, *supra* note 59 at 41.

63 *Ibid* at 9, 18.

64 *Ibid* at 9.

65 *Ibid* at 30–31.

e-commerce), and how those gatekeepers have the power to define the rules of competition altogether.[66] The Uber platform and its surge price algorithmic calculations may not necessarily play by the *invisible hand* offer and demand rules but actually set the rules as a price regulator.[67] As Ezrachi and Stucke argue, once in a position of market power, setting surge prices allows both Uber and its drivers to increase their profits at the expense of consumers "all under the guise of "market-clearing" price."[68]

It is therefore in light of this greater *rapprochement* between the effect of firms' data collection and competition law, that big data commercial practices including APP, will need to be reassessed altogether, with a yet undefined renewed role for competition law and policy.[69]

C) Consumer Law

This section looks at general consumer protection statutes, common law doctrines, with some reference to *Code Civil* provisions that may affect pricing terms and APP. More specifically, it applies the general principles derived from pre-contractual obligations (with respect to representations and notification of terms), and the doctrine of unconscionability (lésion, and abusive clauses in the civil law). Other than industry-specific regulation,[70] and consumer protection statutory provisions on price gouging, the actual price charged is largely left unregulated and left to the freedom of contracting parties.[71] And yet, some of the doctrines and principles analysed here may call in question the legality of APP, not so much as it regards the acceptability of the price itself, but because of the circumstances surrounding how the contract pricing term was arrived at and presented to the buyer.

---

66 *Ibid* at 30.

67 Ezrachi & Stucke, *supra* note 3 at 211–12.

68 *Ibid* at 211.

69 This renewed role is increasingly veered toward safeguarding the public interest beyond the mere protection of competitive markets and deceptive commercial practices: See ISED, Future of Competition Policy, *supra* note 59, Slaughter et al, *supra* note 42.

70 See Karton, *supra* note 23 (on specific pricing regulation per industry sector).

71 *Ibid* at 3–7 (for a discussion of the application of Canadian common law doctrines to contract pricing terms). This is consistent with the common law doctrine of consideration or the requirement of the exchange of value without judgement on the value exchanged between the parties: see *Thomas v Thomas* (1842), 2 QB 851, [1842] 2 WLUK 19.

1) Pre-contractual Obligations, Notification of Terms, and Representations

Precontractual misrepresentations, or the failure to bring important contract terms to the attention of the buyer, may lead to the invalidity of the contract (or contract term(s)), whether under the common law, the *Code Civil* or consumer protection statutes. In common law contracts, for a claim of misrepresentation to be successful, there needs to be a false statement that is material to enter the contract.[72] Exceptionally, omission of important facts may amount to a misrepresentation.[73] Misrepresentation may be difficult to prove with respect to personalized pricing. This could occur when the buyer is misled to believe that the same product is offered at the same price to all buyers, i.e., a misstatement given that the price was personalised. Even with this false statement, the buyer would still have to establish that this was a material factor to enter the contract.[74] It is debatable, but not implausible that uniformity of price is material to the buyer, especially if a representation was made to that effect and turned out to be false, as going against the reasonable expectation of the buyer.

It is less clear that an omission to inform the buyer about personalized pricing amounts to a misrepresentation, given the reluctance in common law to treat omissions or silence as misrepresentations.[75] The issue here is that the omission does not pertain to the accuracy of the price itself, but to the price relative to other buyers, external to the relevant specific transaction. It becomes a question of materiality of both the omission and how it affects the buyer's decision to enter the contract. It also boils down to the objective assessment of the reasonable expectation of the buyer. At a time where online dynamic pricing prevails, and whereby there is *per se* no obligation in law to charge uniform prices to buyers (unless a different price is charged on the basis of prohibited grounds of discrimination

---

72 *Redgrave v Hurd* (1881), 20 Ch D 1 (CA), [1881] 11 WLUK 98: misrepresentation occurs when the supplier made a statement that was false, that was material, in which case there is a presumption that it induced the claimant to conclude the contract. The buyer may ask rescission of a contract and restitution. Misrepresentation may be innocent, negligent or fraudulent, and in the two latter cases, amounts to a tort that may also give rise to damages: John D. McCamus, *The Law of Contracts*, 3rd ed (Toronto: Irwin Law Inc., 2020) at 359–401, 730–41 (on the doctrine of misrepresentation in Canadian contract law, common law jurisdictions).

73 See e.g. *Bank of British Columbia v Wren Developments Ltd. et al*, 1973 CanLII 1153 (BCSC), McCamus, *supra* note 72 at 366–68 (about how the traditional rule at the common law is that a party is not required to disclose material facts at contract formation with very few exceptions).

74 *Ibid*. See also Miller, *supra* note 6 at 76–78 (on the application of misrepresentation to price discrimination in US contract law).

75 See *supra* note 73.

under human rights codes),[76] arguing that the failure to mention that the prices are personalized is a misrepresentation that may progressively become weaker as dynamic e-commerce pricing practices become more commonplace.

Misrepresentation might occur in other cases, if e.g., the supplier represents that they comply with privacy law (or such compliance can be implied) while their use of personal data in setting the price violates personal data protection law.[77] But again, the buyer would need to establish that this was a material factor that induced them to conclude the contract. These are some of the scenarios under which the practice of personalized pricing could be attacked on the ground that it amounts to misrepresentation. In all cases, misrepresentation leads to a deception vitiating an otherwise binding contract, and allows the buyer to claim rescission, restitution, and depending on the nature of the misrepresentation, damages.[78] A pre-contractual representation may also amount to a contractual warranty in some circumstances, the breach of which gives rise to all remedies available for breach of contract.[79]

Variations of the doctrine of misrepresentation have been codified in provincial consumer protection statutes, alleviating some of the hurdles toward a successful claim at common law. The statutes make it an unfair practice for a person to make a misleading or deceptive representation in a consumer contract context.[80] The statutes typically contain non-exhaustive lists of prohibited representations, some of which pertain to price terms, e.g., misrepresenting a price advantage, the total value of instalments, a sale, or that the product is sold "at supplier's cost", none

---

76 *Canadian Human Rights Act*, RSC 1985, c H-6. At the provincial level, see e.g. *Ontario Human Rights Code*, RSO 1990, c H-19, *Charte des droits et libertés de la personne*, CQLR c C-12.

77 See e.g. *Tocco v Bell Mobility Inc.*, 2019 ONSC 2916 at para 31 (on the claim of misrepresentation for misuse of personal data in the consumer class action certification procedure, where the Privacy Commissioner had found service supplier Bell Mobility to violate *PIPEDA*, *infra* note 109).

78 See *supra* note 72. On a related idea to misrepresentation and APP see Noga Blickstein Shchory, "Information Asymmetries in e-Commerce: the Challenge of Credence Qualities" (2020) 20 J High Tech L 1 (on the credence qualities of personalized pricing. The lack of transparency concerning credence goods or services gives rise to greater consumer protection concerns).

79 McCamus, *supra* note 72 at 786–92.

80 *Consumer Protection Act*, *2002*, SO 2002, c 30, s 14 [*OCPA*]; *Consumer Protection Act, 2023*, SO 2023, c 23, s 8 [*OCPA* 2023] (as of the finalization date of this article, the *OCPA* 2023 received royal assent on December 6, 2023, but has not yet come into force); *Loi sur la Protection du Consommateur*, CQLR c P-40.1, s 219 [*LPCQ*].

of which directly pertain to personalized pricing.[81] The materiality of those prohibited representations inducing conclusion of the contract is presumed.[82] The consumer may ask for rescission of the contract or other remedies if rescission is not available.[83] More generally, the omission or ambiguity around a material fact also constitutes a misrepresentation giving rise to the same remedies.[84] Whether the failure to disclose in a consumer contract that the offered price is personalized is a *material fact* has not been tested in court. As per the above discussion on the common law doctrine of misrepresentation, it is debatable whether this would be the case. Given the consumer protection objectives of these statutes and the focus on information disclosure, the argument that failure to inform consumers that prices are personalised is material, and hence an unfair practice, might have more success than with respect to common law misrepresentation. The European Union, Council Directive 2019/2161 requires suppliers to specifically disclose when "the price was personalized on the basis of automated decision-making".[85] These recent changes to strengthen consumer protection in the EU lend support to the materiality of disclosing personalized pricing in consumer contracts. As we discuss next, while the common law reasonable notice doctrine and consumer protection statutes require that important information be brought to the attention of buyers, they are not explicit with respect to automated price personalization.

Other pre-contractual requirements relevant to APP concern the level of disclosure of contract terms in non-negotiated standard form agreements, also referred to as contracts of adhesion. While the validity of contracts of adhesion, including online standard form agreements has long been recognized,[86] the common law doctrine of reasonable notice

---

81 *OCPA*, *supra* note 80, s 14(2)(11); *OCPA* 2023, *supra* note 80, s 8(2)(13),(16); *LPCQ*, *supra* note 80, ss 224–225, 232.

82 *LPCQ*, *supra* note 80, s 253; *OCPA*, *supra* note 80, ss 15,17–18.

83 *OCPA*, *supra* note 80, s 18; *OCPA* 2023, *supra* note 80, s 49; *LPCQ*, *supra* note 80, ss 270–271.

84 *OPCA*, *supra* note 80, s 14(2)(14); *OCPA* 2023, *supra* note 80, s 8(2)17; *LPCQ*, *supra* note 80, s 228.

85 EU, *Directive 2019/2161 of the European Parliament and of the Council of 27 November 2019 amending Council Directive 93/13/EEC and Directives 98/6/EC, 2005/29/EC and 2011/83/EU of the European Parliament and of the Council as regards the better enforcement and modernisation of Union consumer protection rules*, [2019] OJ, L 328/7, at art 4(4)(a)(ii) [EU *Directive* 2019/2161]. The remedy is unenforceability of contract: EU, *Directive 2011/83/EU of the European Parliament and of the Council of 25 October 2011 on consumer rights*, [2011] OJ, L 304/64 at art 6(1).

86 *Thornton v Shoe Lane Parking Ltd*., [1971] 2 QB 163 (EWCA), 2 WLR 585 (referring to the old railway ticket cases); *Interfoto Picture Library Ltd. v Stiletto Visual Programmes Ltd*., [1989] 1 QB 433 (EWCA); *Seidel v TELUS Communications Inc*., 2011 SCC 15 at para 2.

requires that onerous terms be sufficiently brought to the attention of the adhering party for those terms to be binding. Onerous terms include terms limiting the liability of the supplier, or that the adhering party would not reasonably expect given the nature and purpose of the agreement.[87] While it is debatable that price personalisation is a material fact that ought to be disclosed in consumer contracts for the price to be binding on the buyer,[88] it might be an even bigger stretch to argue that a personalized price amounts to an onerous term that ought to be specifically brought to the attention of the buyer under the common law doctrine of reasonable notice.[89] One could argue that the collection and processing of personal data involved beneath APP, unbeknownst to buyers, is indeed an onerous commercial practice. In that light, prices set through APP would have to be specifically brought to the attention of the adhering party to be binding. This would be a novel application of the common law doctrine of reasonable notice that ties into the requirement of meaningful consent in personal data protection law.[90] For consumer contracts, the information disclosure required under the relevant statutes relate to listed terms, which may vary depending on the type of contract.[91] If complied with, such general disclosure requirements do not raise particular issues regarding the legality of APP. As noted earlier, unlike the European Union, there is no specific explicit requirement in Canadian commercial law for suppliers to disclose that they resort to APP.[92]

---

87 *Tilden Rent-A-Car Co. v Clendenning*, 1978 CanLII 1446 (ONCA); *Karroll v Silver Star Mountain Resorts Ltd.*, 1988 CanLII 3294 (BCSC).

88 See *supra* notes 72–74.

89 See *supra* note 87.

90 See below subsection 4B) "Valid Consent for the use of Personal Information".

91 *OCPA*, *supra* note 80, ss 5, 38(1); *OCPA* 2023, *supra* note 80, s 17, 39; *LPCQ*, *supra* note 80, ss 54.4 (*in fine* and in particular paras e) f) g), which relate specifically to pricing terms); ss 223, 223.1. Failure to comply with information disclosure requirements allows the buyer to ask for rescission and restitution: *OCPA*, *Ibid*, s 40; *LPCQ*, *Ibid*, ss 54.8, 54.13.

92 See *supra* note 85.

2) Unconscionability, Lésion, and Abusive Clauses

The common law doctrine of unconscionability (in the Québec civil law, of lésion,[93] and abusive clauses[94]), along with statutory prohibitions against "blacklist" unfair commercial practices in consumer contracts,[95] allow courts to significantly limit freedom of contract where one party takes undue advantage of the inequality in bargaining power against the weakness of the other party.[96] In such cases, the weaker party may ask for rescission of the contract or other remedies.[97] Traditionally more limited to situations where one party took advantage of a serious weakness of another party (e.g., illness, low education level, etc.) vitiating the contract at the procedural level, recent decisions by the Supreme Court of Canada confirm a broader application of the common law doctrine of unconscionability at the substantive level, holding non-negotiated standard contract clauses to be unenforceable, without necessarily involving capacity issues of the weaker party at the outset.[98] This broader application of unconscionability is of particular relevance to APP as this pricing practice is often deployed through non-negotiated standard form consumer contracts. There is a growing recognition and understanding of

---

93 Arts 1405–1406 CCQ (lésion in civil law is limited to minors and to persons under tutorship or under a protection mandate); *LPCQ*, *supra* note 80, s 8 (allowing rescission and other remedies in consumer contracts "where the disproportion between the respective obligations of the parties is so great as to amount to exploitation of the consumer or where the obligation of the consumer is excessive, harsh or unconscionable"). See Marie-Claude Desjardins & Nathalie Vézina, "Le prix dans les contrats de consommation, les contrats d'adhésion et les contrats réglementés—pouvoir d'intervention des tribunaux et autres modes de contrôle des prix en droit québécois" in *Control of Price Related Terms in Standard Form Contracts*, ed by Yesim M. Atamer & Pascal Pichonnaz (Basel: Springer International Publishing, 2020) 232 at 242–244 (for a discussion on the general regime of lésion in the CCQ).

94 Art 1437 CCQ (prohibiting abusive clauses in consumer contracts and in contracts of adhesion, i.e. a "clause which is excessively and unreasonably detrimental to the consumer or the adhering party and is therefore not in good faith; in particular, a clause which so departs from the fundamental obligations arising from the rules normally governing the contract that it changes the nature of the contract …").

95 *OCPA*, *supra* note 80, ss 15, 17 (unconscionable representations as prohibited unfair practices with a non-exhaustive list of factors to consider in assessing unconscionability); *OCPA* 2023, *supra* note 80, s 9.

96 *Uber Technologies Inc. v Heller*, 2020 SCC 16 (unconscionability "requires both an inequality of bargaining power and a resulting improvident bargain" at para 65) [*Uber*].

97 *Uber*, *supra* note 96 at para 99; *OCPA*, *supra* note 80, s 18; *OCPA* 2023, *supra* note 80, s 49; Art 1407 CCQ.

98 *Uber*, *supra* note 96; *Douez v Facebook*, 2017 SCC 33 at paras 114–23, 131–35 (separate reasons for majority by Justice Abella) [*Douez*]; *Titus v William F. Cooke Enterprises Inc.*, 2007 ONCA 573 (on the previous narrower application of the common law doctrine of unconscionability rejected by the Supreme Court in *Uber*, *Ibid* at para 82).

the inherent imbalance of bargaining power and asymmetry of knowledge that prevails in online standard term agreements that consumers "agree to" without understanding or reading them.[99]

Price gouging comes to mind as an unconscionable commercial practice where the buyer can ask for rescission of a consumer contract where "the price grossly exceeds the price at which similar goods or services are readily available to like consumers."[100] Uber algorithmic surging price practices for car driver rides have been criticized for causing serious harm to consumers.[101]

Aside from cases of price gouging, could APP amount to an unconscionable practice, particularly in consumer contracts where it involves the use of consumers' personal information, often surreptitiously and to their detriment? (I.e., by targeting each consumer's maximum willingness to pay, hence reducing individual and overall consumer surplus). There are diverging views among scholars as to when and how discriminatory pricing may amount to an unconscionable practice.[102] While the Supreme Court has broadened the application of the doctrine of unconscionability, emphasizing inequality of bargaining power (the first part of the test) in non-negotiated standard term contracts,[103] it is less clear that APP leads to an *improvident bargain* (the second part of the test) at the individual level, i.e., a bargain that "unduly advantages the stronger party or unduly disadvantages the more vulnerable".[104] The argument that APP is an unconscionable commercial practice may have

---

99 Margaret Jane Radin, *Boilerplate the Fine Print, Vanishing Rights, and the Rule of Law*, (Princeton University Press, 2013) at 3–18; Shirly Levy, "Fixing Standard-Form Contracts" (2023) 91:3 U Cin L Rev 789 at 794–802.

100 *OCPA*, *supra* note 80, ss 15(2)(b), 18; see also *OCPA* 2023, *supra* note 80, s 9(2)2.

101 See Ramsi A. Woodcock, "The Efficient Queue and the Case Against Dynamic Pricing" (2020) 105 Iowa L Rev 1759 (on the harmfulness for consumers of dynamic pricing including surge price tactics, recommending anti-trust government bodies to intervene and ban dynamic pricing).

102 Miller, *supra* note 6 at 82–84 (discussing possible arguments of unconscionability with respect to personalized pricing as being rather weak and inconclusive); Mark Klock, "Unconscionability and Price Discrimination" (2002) 69 Tenn L Rev 317 (suggesting a redefined and narrow application of the doctrine of unconscionability based on market failure, linking competition policy to public policy, and under which any price discrimination that is not justified by cost (or by quality) is only possible in non-competitive markets, and that all price discrimination that is not justified by costs is unconscionable); See also Graef, *supra* note 29 at 11 (concluding that personalised pricing would not violate EU consumer protection law on the basis that adequacy of price is not a ground to assess the unfair nature of a commercial practice under the relevant applicable EU directives).

103 *Uber*, *supra* note 96; *Douez*, *supra* note 98 (separate reasons for majority by Justice Abella).

104 *Uber*, *supra* note 96 at para 74.

more force when the automated mass-market practice is viewed broadly, as one that unduly advantages the stronger party.[105] The broader effects of a commercial practice may be more suited to a competition law analysis than when applying the doctrine of unconscionability or similar common law doctrines.[106] In the end, what is more problematic about APP is not necessarily the price term it leads to, but how it is arrived at. In that light, the indiscriminate use of personal information to set the price, often unbeknownst to the buyer might be what unduly disadvantages the more vulnerable.[107]

3) Assessment

The price charged for goods or services in a supply agreement is largely left to freedom of contract at common law and in the civil law, except for some specific industries, and some tighter requirements surrounding price terms in consumer contracts. Our analysis of APP with respect to pre-contractual obligations and representations, and of the doctrine of unconscionability (lésion and abusive terms in civil law) showed instances where under the specific circumstances enumerated above, price terms or the contract could be rescinded. Other than those specific scenarios, there is no definitive argument that the commercial practice of APP contravenes per se to these doctrines, principles, or consumer protection statutory provisions.

APP might give rise to breach of express or implied contract terms in some cases, including through the application of personal data protection law to this commercial practice.[108]

4. Personal Data Protection Law

Federal and provincial personal data protection statutes govern how the private sector may collect, use, and disclose personal information in the course of a commercial activity. The federal *Personal Information*

---

105 See also *OCPA*, *supra* note 80, ss 15(2)(c), (e) (about unconscionable representations when "(c) … consumer is unable to receive a substantial benefit from the subject-matter of the representation" or "(e) … consumer transaction is excessively one-sided in favour of someone other than the consumer); *OCPA* 2023, *supra* note 80, ss (2)3, 6.

106 See *supra* section 3B)1) "Macro-market Anti-competitive Practices".

107 *Uber*, *supra* note 96 at para 74.

108 See below section 5 "Conclusion: A New Era for Price Regulation in the Digital Marketplace? Consumer Law and Competition Law Meet Personal Data Protection Law".

Protection and Electronic Documents Act [*PIPEDA*],[109] applies in all provinces except provinces with equivalent legislation,[110] to federally regulated organizations (e.g., banks, telecommunications, railway, air transportation companies), and to all relevant interprovincial and international transactions.[111] This part focuses on the application of *PIPEDA*, while also taking into account Bill C-27 *Consumer Privacy Protection Act*[112] [Bill C-27 *CPPA*], as ongoing legislative reform aims toward a complete overhaul of *PIPEDA*. Different statutes not relevant to APP govern how various levels of government may handle personal information.[113]

When assessing the legality of APP under *PIPEDA*, we ask whether a supplier is entitled to collect, use, and disclose the personal information of a potential customer for the purpose of getting as close as possible to their maximum willingness to pay. The use of personal data required for APP would generally be considered personal information under *PIPEDA*.[114] This includes information that is publicly available with some limited exceptions.[115]

The parameters within which firms may use personal information rest on two basic principles that are interrelated: valid consent, and the

---

109 *Personal Information Protection and Electronic Documents Act*, SC 2000, c 5 [*PIPEDA*] ("Personal Information means information about an identifiable individual", s 2(1)).

110 I.e. Alberta, British Columbia, and Québec. Neither does *PIPEDA* apply to personal health information in Ontario, New Brunswick, Nova Scotia, and Newfoundland and Labrador.

111 Barbara von Tigerstrom, *Information & Privacy Law in Canada* (Toronto: Irwin Law Inc., 2020) at 339–66 (for an overview of the regulation of the collection, use, and disclosure of personal information in federal and provincial statutes applicable to the private sector).

112 Bill C-27, *Digital Charter Implementation Act*, 1st Sess, 44th Parl [Bill C-27] (if enacted, leading to the implementation of the *Consumer Privacy Protection Act [CPPA]*, *the Personal Information and Data Protection Tribunal Act* [*DPTA*], and *the Artificial Intelligence and Data Act* [*AIDA*]). At the date of completion of this article, Bill C-27 has not yet passed into law.

113 Canada's *Privacy Act*, RSC 1985, c P-21 and provincial statutes applying to the public sector, e.g. *Freedom of Information and Protection of Privacy Act*, RSO 1990, c F-31.

114 *PIPEDA*, *supra* note 109 ("Personal Information means information about an identifiable individual", s 2(1)); Bill C-27 *CPPA*, *supra* note 112, s 2(1) (retaining the same definition of "Personal Information" as in *PIPEDA*).

115 *PIPEDA*, *supra* note 109, s 7(1)(d) (exception to requirement of knowledge or consent under *PIPEDA* for publicly available information is a narrow list that includes e.g. telephone or professional or business directories, but does not include information available on social media: *Regulations Specifying Publicly Available Information*, SOR/2001-7, s 1); Bill C-27 *CPPA*, *supra* note 112, s 51.

reasonableness of the purpose for which personal information is used.[116] Our analysis will proceed in three parts. First, we discuss the implications of the quasi-constitutional status of privacy in Canada linking personal data protection to a human right. Second, we explore the extent to which an individual can validly consent under *PIPEDA* to their personal information being collected and used for the purpose of APP. Third, we ask whether such collection would meet the requirement of what a reasonable person would expect in the circumstances.

A) The Quasi-constitutional Status of Privacy and Personal Data Protection

Unlike other jurisdictions including the EU,[117] the *Canadian Charter of Rights and Freedoms*[118] [*Canadian Charter*], which applies to various levels of Governments and other public sector entities, does not provide general protection of privacy as a fundamental right or freedom. The constitutional protection of privacy is recognized under section 8, the right to be secure against unreasonable search or seizure, and to a lesser extent under section 7, the right to life, liberty, and security of the person.[119] At the provincial level, the Québec *Charter of Human Rights and Freedoms* does refer to the general right to privacy as a human right.[120]

The jurisprudence by the Supreme Court of Canada on the right to be secure against unreasonable search or seizure has been foundational to the elaboration of the right to privacy in Canadian public and private law.[121] While the *Canadian Charter* does not apply to disputes between private parties, the Supreme Court has often referred to the constitutional

---

116 *PIPEDA*, *supra* note 109, s 5(3) (constraining "only for purposes that a reasonable person would consider are appropriate in the circumstances."), s 6.1 (on valid consent requiring that the person would understand the nature, purpose, and consequences of the handling of personal information to which they are consenting), cl 4.2 of Schedule 1 (requiring organisation to disclose purpose for handling of personal information), cl 4.3 of Schedule 1 (stating required levels of consent for handling of personal information).

117 Council of Europe, *European Convention for the Protection of Human Rights and Fundamental Freedoms, as amended by Protocols Nos 11 and 14*, (1950) at art 8; EU, *Charter of Fundamental Rights of the European Union*, [2012] OJ, C 326/391 at arts 7–8.

118 *Canadian Charter of Rights and Freedoms*, s 7, Part 1 of the *Constitution Act, 1982*, being Schedule B to the *Canada Act 1982* (UK), 1982, c 11 [*Canadian Charter*].

119 See von Tigerstrom, *supra* note 111 at 7–24 (on the Canadian Charter information and privacy law framework).

120 *Charte des Droits et Libertés de la Personne*, *supra* note 76, s 4–5, 9 (applies to private and public entities in Québec; does not apply to public or private institutions under Federal authority).

121 See e.g. *Jones v Tsige* 2012 ONCA 32 at paras 39–46 (on the protection of privacy in the *Canadian Charter*, and on the recognition of common law privacy related torts based on informational privacy, more specifically the tort of intrusion upon seclusion).

protection of privacy as a *Canadian Charter* value that should guide the interpretation of private law.[122] The Supreme Court has also referred to the protection of privacy as a quasi-constitutional right in applying privacy laws to the private sector.[123] Similarly, the Office of the Privacy Commissioner of Canada has declared on several occasions that personal data protection should be treated as a human right, relying on international instruments and Canadian jurisprudence on privacy.[124]

When *PIPEDA* was enacted in 2000, it was viewed and justified as falling under the federal government's general trade and commerce power under the Constitution. The impetus for this enactment at the federal level came from the EU, one of Canada's major trading partners, to have a proper data protection law regime in place. More than two decades later, the current personal data protection legislative reform efforts link personal data protection to fundamental rights and freedoms in Canada and in international instruments, with Bill C-27 *CPPA* making this connection in its preamble.[125] While Bill C-27 *CPPA* is replete with personal data commodification undertones (referencing the importance of innovation and of the digital and data-driven economy), connecting personal data protection legislation to human rights could have important

---

[122] *Ibid* at paras 43, 45–46 (citing several Supreme Court decisions as support for the recognition of common law privacy-related torts).

[123] *Douez*, *supra* note 98 at paras 59, 105 (citing earlier Supreme Court decisions). See also *Privacy Commissioner of Canada v Facebook, Inc.*, 2023 FC 533 at para 51 (acknowledging the quasi-constitutional status of *PIPEDA*; and dismissing the Privacy Commissioner's application alleging that Facebook had breached *PIPEDA* by failing to obtain valid consent through its practices of sharing Facebook users' personal information with third-party application providers, for lack of evidence and failing to discharge its burden of proof, referring to an "evidentiary vacuum": *Ibid* at para 71); decision on appeal: FCA Docket A-129-23.

[124] See e.g. Office of the Privacy Comissioner of Canada, "Commissioner: Reform bill "a step back overall" for privacy" (11 May 2021), online: <https://tinyurl.com/46c4a6zz> [perma.cc/KX5A-YKWM] (criticizing Bill C-11 predecessor to Bill C-27 *CPPA* in the ongoing legislative reform on personal data protection in the private sector, and that it "should be amended to adopt a rights-based framework that would entrench privacy as a human right and as an essential element for the exercise of other fundamental rights"); Office of the Privacy Commissioner of Canada, "Submission of the Office of the Privacy Commissioner of Canada on Bill C-27, the Digital Charter Implementation Act, 2022" (26 April 2023), online: <https://tinyurl.com/mrxwkm5r> [perma.cc/N2XY-9T4C].

[125] Bill C-27 *CPPA*, *supra* note 112 (Preamble: "… the protection of the privacy interests of individuals with respect to their personal information is essential to individual autonomy and dignity and to the full enjoyment of fundamental rights and freedoms in Canada").

consequences on the future scope of this legal regime when set against obvious commercial trade interests.[126]

B) Valid Consent for the use of Personal Information

The protection of personal information under *PIPEDA* rests in large part on the requirement of *valid consent*, as a mean to preserve individual autonomy. Valid consent is an elusive concept in the realm of standard form agreements and privacy terms are no exception. Lack of attention to those terms, lack of understanding even when paying attention to those terms, asymmetry of bargaining power, a lack of choice about agreeing to those terms, challenge the traditional understanding of consent in the context of contracts of adhesion.[127] Additionally, the privacy safeguards conferred through obtaining valid consent largely depend on what the law allows firms to make us consent to. A too heavy reliance on obtaining valid consent as main regulatory gatekeeper to the protection of personal data is bound to be structurally defective given firms interests and economic stakes toward personal data collection. Consent then becomes the conduit to extraction rather than protection of personal information.[128]

Legislative change, court decisions and guidelines by The Office of the Privacy Commissioner of Canada (OPCC) have progressively led to strengthening the valid consent requirement in *PIPEDA*. For instance since 2015, *PIPEDA* provides that consent is only valid if "it is reasonable to expect that an individual … would understand the nature, purpose and consequences of the collection, use or disclosure of the personal information", tying consent to clarity of disclosure of the relevant information.[129] And while valid consent may be implied under *PIPEDA*,[130] in *Royal Bank of Canada v Trang*, [131] the Supreme Court stated that

---

126 Teresa Scassa, "Bill C-27 and a human rights-based approach to data protection" (2 August 2022), online: <https://tinyurl.com/4avh4z9j> [perma.cc/HYA5-KU4L] (for a critique of Bill-C27 for failing to take a firmer approach to treating personal data protection as a human right, despite reference to human rights in its Preamble).

127 *Douez*, *supra* note 98 at para 99 (Justice Abella concurring reasons for the majority).

128 Lisa M. Austin, "Enough About Me: Why Privacy is About Power, Not Consent (or Harm)" in *A World without Privacy: What Can/Should Law Do?*, ed by Austin Sarat (Cambridge: Cambridge University Press, 2014) at 131 (section 2. "Consent and its discontents" highlighting various critiques of consent as regulatory tool). See also Trudo Lemmens & Lisa Austin, "Privacy, Consent, and Governance" in *New Challenges for Biobanks: Ethics, Law and Governance*, ed by Kris Dierickx & Pascal Borry (Antwerpen: Intersentia, 2009) at 111.

129 *PIPEDA*, *supra* note 109, s 6.1.

130 *Ibid*, cl 4.3.6, schedule 1.

131 *Royal Bank of Canada v Trang*, 2016 SCC 50 [*Trang*].

informed consent is foundational to *PIPEDA* and that the *Act* generally requires express consent.[132] This led the OPCC to update its guidelines on meaningful consent and to clarify when express consent was required. These guidelines further provide that express consent is generally required when the information is sensitive; its collection, use or disclosure is outside the reasonable expectations of the individual, or it "creates a meaningful residual risk of significant harm".[133] Express consent is set to remain the general rule of personal data protection in Canada.[134]

Opting-out mechanisms whereby personal information is collected, used, or disclosed unless individuals actively refuse, may still meet the requirements of obtaining valid consent to the extent that individuals are informed of the ability to opt out.[135] Furthermore, obtaining consent to the collection, use or disclosure of personal data cannot be tied as a precondition to supply a product or service beyond what the firm is required to do for explicitly specified and legitimate purposes.[136]

Under what conditions can valid consent be obtained for use of personal information for APP, i.e., to assess a potential customer's maximum willingness to pay? We argue that valid meaningful consent can never be obtained with respect to the business practice of APP for the reasons that follow.

First, APP requires express consent, which is the general rule under *PIPEDA*.[137] This contrasts with instances where consent can be implied,[138]

---

[132] *Ibid* at para 23 (unanimous judgment by Justice Côté).

[133] Office of the Privacy Commisioner of Canada, "Guidelines for obtaining meaningful consent" (May 2018, revised 13 August 2021) online: <https://tinyurl.com/53xb5bk9> [perma.cc/5VZN-K4GK] [OPCC Consent Guidelines].

[134] Bill C-27 *CPPA*, *supra* note 112, ss 15(1),(3)–(4), 52(4) (stating that valid consent requires disclosure of purpose, of personal information collected, and of consequences of collection).

[135] Office of the Privacy Commissioner of Canada, "Interpretation bulletin: Form of Consent" (March 2014, updated 11 December 2015, under review) <https://tinyurl.com/5z9y5ft3> [perma.cc/Q5X2-NJMX]; see also *Englander v Telus Communications inc.*, 2004 FCA 387 at para 65 (where the Federal Court of Appeal held that no valid consent had been given for the use of personal information in various telephone directories as consumers had not been given the clear option to opt out; rather, they had to ask on their own).

[136] *PIPEDA, supra* note 109, cl 4.3.3, schedule 1; see Eloise Gratton "Personalization, Analytics, and Sponsored Services: The Challenges of Applying *PIPEDA* to Online Tracking and Profiling Activities" (2010) 8:2 CJLT 288 at 308–11.

[137] See *supra* notes 130–32.

[138] *PIPEDA*, *supra* note 109, cl 4.3.6, schedule 1 (stating that consent may be implied when it pertains to less sensitive information).

or is not necessary,[139] e.g., collecting an individual's address to send a parcel, or an individual's phone number as an account back-up security tool. Personal data sets of profiles required for price personalization when viewed as a whole, constitute sensitive information for which express consent is required.[140] Such data sets of profiles provide information about an individual's demographics, preferences, purchasing and other habits, friends, networks, political, or other affiliations over which an individual understandably wants to retain control. Furthermore, the use, sharing, or public release of such data sets or profiles could cause significant harm, e.g., reputational or personal safety even, potential for serious harm being another element for which express consent is required.[141] And last but not least, there are strong arguments to the effect that the use of personal information for personalized pricing purposes would be outside the reasonable expectations of the individual.[142]

Even if a firm would seek the express consent to the use of personal data for APP, such express consent cannot be validly obtained. One of the essential features of valid consent is that it is informed.[143] The law sets a reasonable expectation that an individual "would understand the nature, purpose and consequences of the … use … of the personal information."[144] This requires transparency of the nature and breadth of the collection, use, and disclosure of personal information, as well as a clear explanation of the ends for which the personal information will be used.[145]

In the best-case scenario of transparency and clarity about the firm's use of personal information to personalize prices, there are important substantive and practical considerations to obtaining valid consent. First, transparency about the personal information being used requires the firm's disclosure of its nature, which includes the magnitude of the collection: details about which personal information, over which period, and the sources or third parties involved. With APP, such personal information is typically over and above the personal information voluntarily provided

---

139 Bill C-27 *CPPA*, *supra* note 112, s 18(1)–(2) (providing exceptions where express consent is not required when related to the provision of goods or services or to network security and product safety, as long as they are not for "behavioral influencing" purposes).

140 OPCC Consent Guidelines, *supra* note 133.

141 *Ibid*.

142 *Ibid* (reasonable expectations being one of the parameters to assess the need of obtaining express consent).

143 *Trang*, *supra* note 131 at para 23.

144 *PIPEDA*, *supra* note 109, s 6.1.

145 OPCC Consent Guidelines, *supra* note 133; Bill C-27 *CPPA*, *supra* note 112, s 15(3) (providing that valid consent requires: disclosure of purpose, of personal information collected and of consequences of collection).

by the individual when purchasing a good or service.[146] Assuming that the disclosure is such that an individual would understand the full nature of the personal information collected, it would likely (and rightly so) alarm most individuals paying attention to such disclosure. This author has argued elsewhere that disclosure requirements on the extent of the personal information collected for APP, to the extent a firm would be willing to respect and follow it, would deter such firm from resorting to APP altogether.[147] This also ties to why consumer surveys repeatedly show an aversion to personalized pricing.[148] It would also involve third parties with which the firm may have confidential undertakings against the disclosure of where the personal information comes from.

Valid consent also requires that an individual understands the purpose and consequences of the use of their personal information. A general or vague statement that personal data are collected to assist with the adequate selection of contract terms (referencing here the price), etc. would in my view, not allow the consumer to understand the purpose for which the firm collects the personal information. There are no two ways to coat the purpose of APP: firms use personal information to set prices that will get as closely as possible to consumers' maximum willingness to pay, to maximize their profit. The consequences of APP are that individuals will be charged different prices for the exact same good or service on the basis of different personal characteristics which when brought together, single out this consumer. This is in contrast to purchasing goods or services in a brick-and-mortar retail store where personal characteristics generally play no role in singling out a consumer other than e.g., fidelity rebate plans with allocated discounts based on prior purchase volume.[149]

At a substantive level, understanding the consequences of consenting to personal information use for APP means at least understanding whether this will be beneficial or detrimental to the individual. Although there is no consensus on this issue, APP is viewed as likely to be more detrimental than favourable to consumers.[150] Without sophisticated knowledge (of retail pricing, marketing, economics) understanding the consequences (i.e., benefit or detriment) of the use of one's personal information is illusory. This is to be contrasted with use of personal information for purposes that directly benefit the consumer, such as: improving a website's

---

146 Chapdelaine, *supra* note 11 at 9–12 (providing an overview of the online digital footprint and personal information tracked and collected by suppliers, most often unbeknownst to consumers).

147 *Ibid* at 43–44.

148 See *supra* note 18.

149 See *supra* note 12 (about the high possibility that APP are used in brick-and-mortar stores, e.g. "Amazon Go").

150 See *supra* note 42–45 and *infra* note 172.

performance (temporarily storing personal data about use preferences) or increased security of one's account (prompting requests for personal information and passwords). This is also in contrast with the collection of personal information for personalized ads, for which the individual may more easily understand the consequences of disclosing their personal information than for APP. This is not to suggest that all personalized ads or other forms of behavioural business tactics are free from meaningful consent issues or other personal data protection concerns.[151]

At a practical marketing level, it seems unlikely that firms will actually make such required detailed disclosures to fulfill the informed consent requirements of *PIPEDA* and run the risk of seriously upsetting their consumer base. A requirement of full disclosure of APP for personal data protection compliance purposes might in fact act as strong deterrent to resort to the commercial practice of APP altogether, assuming firms' actual compliance with those disclosure requirements.

C) Reasonable Purpose Requirement

PIPEDA provides an overarching safeguard to the protection of personal data by requiring that a firm's use of personal information only be for purposes "that a reasonable person would consider are appropriate in the circumstances".[152] The handling of personal information is always subject to the reasonableness of the purpose of use of personal information, regardless of whether consent is required.[153] Reasonable purpose is assessed contextually and beyond what the individual might subjectively consider reasonable, bringing an objective element to the analysis.[154]

Court decisions and the OPCC Reasonable Purpose Guidelines,[155] provide parameters on what constitutes a reasonable purpose under *PIPEDA*. In *Turner v Telus Communications Inc*,[156] the Federal Court set out the balancing act that needs to take place when assessing the reasonableness of a firm's use of personal information. The Court, in a

---

151 Bill C-27 *CPPA*, *supra* note 112, s 18(1)–(2) (providing that the exception to requiring consent for certain forms of data collection would not apply when the data is collected for "behavioural influencing" purposes); See also subsection 4C) below "Reasonable Purpose Requirement".

152 *PIPEDA*, *supra* note 109, s 5(3).

153 Bill C-27 *CPPA*, *supra* note 112, s 12(1).

154 *Ibid*. *See* Office of the Privacy Commisioner of Canada, "Guidance on Inappropriate Data Practices: Interpretation and Application of Subsection 5(3)" (24 May 2018) online: <https://tinyurl.com/yc632se8> [perma.cc/F7E8-9N8Y] [OPCC Reasonable Purpose Guidelines].

155 *Ibid*.

156 *Turner v Telus Communications Inc.*, 2005 FC 1601, aff'd 2007 FCA 21 [*Turner*].

decision later affirmed by the Federal Court of Appeal, set out the following factors for evaluating whether a firm's purposes are reasonable as required by the Act: (i) the degree of sensitivity of the personal information at issue, (ii) whether the firm's purpose represents a legitimate need or *bona fide* business interest, (iii) whether the collection, use and disclosure would be effective in meeting the firm's needs, (iv) whether there are less invasive means of achieving the same ends at comparable cost and with comparable benefits, and (v) whether the loss of privacy is proportional to the benefits.[157] As noted later by the Federal Court in *Globe24h.com*,[158] the reasonable purpose analysis boils down to the *bona fide* use by the firm as well as the proportionality between the loss of privacy and the benefit gained by the individual for such loss.[159]

The OPCC Reasonable Purpose Guidelines provide further insights into this requirement under *PIPEDA*, including a blacklist of inappropriate purposes of use of personal information.[160] For instance, and not surprisingly, use of personal information that is otherwise unlawful (e.g., against credit lending or landlord-tenant laws), does not meet the reasonable purpose requirement.[161] This would include the use of personal information that contravenes anti-discrimination laws.[162] Of relevance to our discussion on APP, profiling or categorization that leads to unfair or unethical treatment does not meet the reasonable purpose required by *PIPEDA*.[163]

Applying the parameters elaborated by courts, as well as the OPCC Reasonable Purpose Guidelines to APP, firms' collection, use or disclosure of personal information for APP arguably does not constitute a reasonable purpose under *PIPEDA*. Our analysis proceeds on the basis that the handling of personal data falls within the quasi-constitutional right of privacy.[164] Regardless of the greater protection of individuals'

---

157 *Ibid* at para 48; see also *Eastmond v Canadian Pacific Railway*, 2004 FC 852 at para 129; Bill C-27 *CPPA*, *supra* note 112, s 12(2) (enumerating the factors elaborated in *Turner, Ibid*, to assess the reasonableness of the purpose).

158 *A.T. v Globe24h.com*, 2017 FC 114.

159 *Ibid* at para 74 (citing *Turner*, *supra* note 156 at para 48).

160 OPCC Reasonable Purpose Guidelines, *supra* note 154 ("Inappropriate purposes or No-Go Zones", enumerating six practices that constitute unreasonable purposes for the use of personal information).

161 *Ibid*.

162 *Ibid* (referring specifically to discrimination in contravention of human rights laws, i.e. "Profiling or categorization that leads to unfair, unethical or discriminatory treatment contrary to human rights law").

163 *Ibid*.

164 See *supra* subsection 4A) "The Quasi-constitutional Status of Privacy and Personal Data Protection" (on the quasi-constitutional status of privacy and personal data

personal data flowing from this quasi-constitutional status, there are strong arguments that APP does not comply with the requirement of a reasonable purpose under personal data protection law.

APP involves the creation and use of data sets that amount to data subject profiling in varying degrees. Any form of personal data profiling should be viewed as sensitive information overall, and therefore subject to higher scrutiny. The instances in which it can be viewed as serving a bona fide business purpose should remain limited. For instance, subject to anti-discrimination law, personal data profiling for the purpose of providing personal insurance would generally serve such purpose if the insurance company can objectively demonstrate that personal data are collected and used for the purpose of assessing the individual's insurable risk and insurance premium, based on accepted industry standards or demonstrably justifiable actuarial calculations.

The legislative reform underway is instructive on what constitutes a *bona fide* business purpose in assessing the reasonableness of the collection and use of personal information. It sets parameters for the collection and use of personal information without the individual's consent or knowledge.[165] Such purposes pertain to "an activity that is necessary to provide a product or service that the individual has requested from the organization", or for the product or service's safety, or the organization network security.[166] In all cases, the personal information should not be collected with the aim to influence the individual's behaviour or decisions. This suggests a narrow interpretation of *bona fide* business purpose constrained by what a reasonable person would expect.[167]

The purpose of collection, use, and disclosure of personal information for APP is to assess the individual's maximum willingness to pay for a good or service. While this business purpose is undoubtedly serving the interests of the firm toward maximizing profits and that use of personal data sets will become increasingly efficient to achieve this goal, it must also represent legitimate business needs. The unfair advantage gained by the firm's use of personal information for APP calls to question the legitimacy of the practice. By way of comparison, using the street address of an individual to assess the cost of delivery most likely falls in the category of *bona fide* use of such personal information. In contrast, using a

protection).

165 Bill C-27, *supra* note 112, s 18(1)–(2).

166 *Ibid*.

167 *Ibid*. See Teresa Scassa, "Bill C-27's Take on Consent: A Mixed Review" (4 July 2022), online: <https://tinyurl.com/39hea8tz> [perma.cc/EVK6-EWKB] (for a review and critique of business activities for which collection and use of personal information are not subject to knowledge and consent under Bill C-27 *CPPA*, supra note 112).

broad range of personal information to individually assess an individual's maximum willingness to pay, and adjust the price accordingly, would not meet the legitimacy test as easily. Indeed, there are, and have been historically much less personally invasive ways for the firm to maximize profits. Several decades of pricing practice options, (whether in a brick and mortar or online environment) that do not resort to individuals' personal data sets or profiles, offer solid proof to that effect.

The hardest hurdle for APP to meet the reasonable purpose requirement is the proportionality of the loss of privacy compared to the benefits gained by such loss.[168] The data profiling involved in APP is highly intrusive, amounting to significant loss of privacy for the individual concerned. The benefits gained by such loss of privacy have to be measured with respect to the individual. In the case of APP, the benefit of having access to the personal information goes back to the firm. This analysis is further strengthened when we treat personal data protection as a (quasi) human right. Hence, personal information should not be treated as a commodity, and the reasonableness of its use needs to be measured by the interests and benefits gained by the individual in return.

APP as the practice of assessing consumers' maximum willingness to pay is different from other forms of price personalization such as a firm applying price discounts through fidelity programs based on purchase volumes. In this latter case, the collection of personal information gathering prior purchases for the purpose of applying discounts would likely constitute a purpose that a "reasonable person would consider … appropriate in the circumstances."[169] The legality of price discounts and similar loyalty programs would also depend on compliance with misleading advertising requirements, i.e., not artificially inflating prices leading to discounts.[170]

One could argue that APP is beneficial to some individuals. Given its possible distributive effects, it would allow individuals who would normally not be able to afford a good or service access to it, consumers with a higher willingness to pay "subsidizing" those with a lower one.[171]

---

168 See *supra* notes 155–158.

169 *PIPEDA*, *supra* note 109, s 5(3).

170 See above subsection 3B)2) "Deceptive Marketing Practices".

171 See OECD Competition Committee, *supra* note 5 at 20 (pointing to mixed empirical evidence about the impact of traditional price discrimination on surplus distribution among consumers and producers, citing various studies to that effect); OECD EU Submission, *supra* note 3 at 5–6 ; Organisation for Economic Co-operation and Development, "Personalised Pricing In The Digital Era- Summaries Of Contributions" (27 November 2018), online (pdf): <https://tinyurl.com/bp9mkbf6> [perma.cc/4G3M-EDGG].

This argument is problematic given that APP seeks to get as closely as possible to one's maximum willingness to pay, with the aim of reducing consumer surplus individually and overall. As such, APP is likely to harm more than to benefit consumers as a whole.[172]

For argument's sake, let's assume that APP does have positive distributive effects which directly benefit individuals who would otherwise not be able to pay and be left out of the market. From a reasonable purpose perspective, firms aiming a genuine positive distributive effect through APP would need to specifically advise consumers of such purpose for the collection and use of personal data (and act accordingly). Although this concerns primarily the issue of informed consent, could a program specifically disclosing cross subsidization through pricing to allow more buyers who otherwise could not afford a good or service, meet the reasonable purpose requirement under personal data protection law? In my view, the positive distributive effect goal of this APP business practice and its disclosure would not be sufficient to meet the reasonable purpose test, and the above analysis stands. While this positive distributive goal might slightly increase the bona fide business nature of the purpose, the intrusiveness of the personal information used from all individuals concerned would remain hard to justify. Firms can use other ways to charge lower prices to lower-paying customers by segmenting their market base, without doing so by accessing all consumer personal data profiles. In the end, no reasonable person would view broad access to their personal information for a purpose that would likely work against these individuals' interest (in most instances) to be "appropriate in the circumstances". And this is quite aside from the additional practical hurdle that consumers would unlikely buy into this distributive pricing model to begin with, except perhaps in specific, niche areas.[173]

---

[172] See e.g. Frederik Zuiderveen Borgesius & Joost Poort, "Online Price Discrimination and EU Data Privacy Law" (2017) 40 J of Consumer Pol'y 347 at 355 (about how the trend that APP would tend to reduce consumer surplus while increasing producer surplus overall, could even increase with more sophisticated personalized pricing practices); see OECD EU Submission, *supra* note 3 at 5 (observing that personalized pricing is likely to be more negative to consumers overall and especially with respect to first-degree price discrimination, on the basis of an output-expansion effect (pro-competitive effect) combined with a wealth-transfer effect (anti-competitive effect), the latter being likely to be more pronounced).

[173] See Ezrachi & Stucke, *supra* note 3 at 122 (explaining when discriminatory pricing might be acceptable: if there is a social goal, if it improves the overall product, and if it is transparent).

D) Assessment

The difficulty for individuals to fully comprehend the effects of the collection of their personal information and the level of intrusion that data profiling involves relative to the end goal pursued through APP, lead us to conclude that it will be very difficult for suppliers to obtain valid consent and to meet the reasonable purpose requirement under personal data protection law. This conclusion detracts from previous scholarly analyses that APP would be lawful even under the more stringent personal data protection EU GDPR[174] regime, subject to full disclosure of APP and obtaining valid consent, to the extent that these scholarly assessments suggest that suppliers resorting to APP could actually meet these requirements.[175] In the EU, the acceptability of APP, provided there is explicit disclosure of this commercial practice is further reinforced by EU Directive 2019/2161.[176] Our analysis of APP showed the actual hurdles implicated in obtaining valid consent, and how under the Canadian regime of personal data protection, valid consent is inevitably tied to the reasonableness of the purpose for which personal information is collected and used. We arrive to this conclusion independently of viewing personal data protection as a human right, while acknowledging that such recognition significantly strengthens the arguments that APP does not comply with personal data protection law.

5. Conclusion: A New Era for Price Regulation in the Digital Marketplace? Consumer Law and Competition Law Meet Personal Data Protection Law

Our assessment that the commercial practice of APP does not comply with personal data protection law shifts the paradigm of consumer law.

---

174 EU, *Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)*, [2016] OJ, L 119/1 [EU GDPR].

175 See e.g. Zuiderveen Borgesius & Poort, *supra* note 172 at 356 (describing the effect of applying the EU GDPR to price discrimination as forcing suppliers to disclose in clear and unequivocal terms the practice to their consumers, as opposed to general terms on the collection of personal data); Sears, *supra* note 3 at 20–26 (assessing the legality of online personalized pricing under EU data protection law by fulfilling the requirements of transparency, disclosure, and valid consent). See also Fabrizio Esposito, "The GDPR enshrines the right to the impersonal Price" (2022) 45 Computer L & Security Rev 1 (arguing that consumers have the right to be offered "impersonal prices" under the EU GDPR, *supra* note 174, which flows from valid consent and the right of data subjects to object to the collection of their personal data).

176 *Supra* note 85 (requiring suppliers to specifically disclose when "the price was personalized on the basis of automated decision-making").

It disturbs the so far largely unregulated sphere of how price is set in a consumer agreement. Not so much by putting boundaries on adequate pricing levels, but more with respect to how the price is arrived at. When setting a price, using the personal information of a potential customer to assess their maximum willingness to pay goes against the core principles of valid consent and reasonable purpose under personal data protection law. The quasi-constitutional nature of personal data protection reinforces that conclusion. Personal data protection as a (quasi) human right means that personal information is not tradable at the same level that commodities are in the marketplace. It can be waived only for a benefit to the individual that they can reasonably understand and validly consent to, or a larger bona fide business purpose which in the end also benefits the consumer.

The conclusion that APP does not comply with personal data protection law can further give rise to supplier breach of consumer contracts. For instance, the commercial practice of APP could be a breach of general express warranties that a supplier abides by the privacy law of a given jurisdiction, or similar terms. Additionally, the doctrine of implication of terms is another way by which statutory personal data protection obligations become part of the contract.[177] A finding that by resorting to APP, a supplier also breaches a consumer contract, could bring additional procedural or remedial benefits to a claim of violation of personal data protection law.[178] This is particularly relevant given the paucity of effective remedies under this body of law.[179]

Furthermore, a conclusion that APP does not comply with personal data protection law may change the application of common law doctrines or consumer protection statutes examined earlier. For instance, it shifts the analysis on requirements of reasonable notice or disclosure, as it relates to e.g., the materiality of the practice of APP to the consumer transaction. In other words, it strengthens arguments that APP is a material fact that ought to be disclosed to consumers pursuant to the relevant statutory or common law requirements. The conclusion that APP contravenes to personal data protection law may also strengthen the argument that the commercial practice is unconscionable. The reverse is also true: an unequivocal pronouncement that APP complies with personal data

---

[177] *Machtinger v Hoj Industries Ltd.*, 1992 CanLII 102 (SCC) (laying out the three instances under which terms may be implied in under common law contracts: (i) as a matter of custom or usage, (ii) to give business efficacy to the transaction, and (iii) as a legal incident of particular kind of contract (e.g. employment)).

[178] I.e. through the application of statutes of limitations, or other procedural advantages in establishing the breach of contract claim, as well as regarding the scope of the remedies available, in contrast with violation of personal data protection law.

[179] This is the case under *PIPEDA*, *supra* note 109. Bill C-27 *DPTA*, *supra* note 112 would introduce additional fines and remedies for violations under Bill C-27, *ibid*.

protection law would weaken any argument that APP contravenes to the various common law, civil law principles, or consumer protection statutes analysed earlier.

Beyond the impact of personal data protection law on APP in consumer contracts, the re-examination and reform of competition law in the digital marketplace currently under way, could change the assessment presented here. That is, as it concerns the legality of APP from a competition law perspective in business-to-business transactions as well as for consumer contracts. Findings of illegality under personal data protection law coupled with findings that APP leads to a decrease in consumer welfare overall, could ignite legal reform addressing the anti-competitive effects of APP and other forms of algorithmic personalization. This would include addressing the unfairness of this practice and how it may erode trust in the marketplace overtime, to the same extent that misleading advertising does.

It is too early to tell what other impact future legislation on artificial intelligence (AI) governance (such as contemplated under Bill C-27),[180] will have on APP. This is particularly true for business-to-business supplier agreements. At this stage, at least for consumer contracts, the personal data protection regime analysed here is more directly pertinent to the regulation of APP.[181]

The present analysis and conclusions regarding APP may be relevant to other business practices involving the collection, use, and disclosure of personal information or business data. The case of so-called dynamic pricing, behavioural advertising or other surreptitious practices come to mind, when suppliers benefit from access to large amounts of personal information or other big data, and of increasingly sophisticated data analytic tools that place consumers or other buyers' online transactions and behaviour under constant surveillance.

---

180 *AIDA, supra* note 112.

181 *Ibid*. If enacted, will impose obligations on suppliers deploying or using AI systems to prevent *inter alia* violations of anti-discrimination law, which is beyond the scope of this article.