PREVENTING THE PERILS OF PERSONALIZED PRICING: A PROPOSED REGULATORY CODE FOR PERSONALIZED PRICING ALGORITHMS

Tristan Montag*

Due to the expanding digital marketplace, more consumers have been, and continue to be, subject to price discrimination, whereby consumers are charged different prices for a similar item sold by the same vendor. To perform price discrimination, sellers implement personalized pricing algorithms ("PPAs"), which use artificial intelligence ("AI") to analyze consumer data to set prices that achieve the maximum amount of profit. The fact that PPAs are benefitting sellers in the digital marketplace suggests that a market failure exists that warrants attention and regulation. Moreover, price discrimination can significantly harm consumer welfare and competition in the digital marketplace, especially when PPAs operate on biased data. However, Canada currently has no regulations against PPAs or price discrimination. This paper provides an overview of PPAs and suggests the implementation of an ex-ante, rules-based regulatory code inspired by the frameworks of the United States and the European Union. By prohibiting the collection and use of personal data, mandating disclosure and consumer consent and requiring ongoing PPA assessments, the Code aims to prevent the perils of personalized pricing in the digital marketplace.

En raison de la croissance du marché numérique, un plus grand nombre de consommateurs sont—et continuent d'être—exposés à des pratiques de discrimination par les prix, selon les-quelles un même vendeur facture des prix différents pour des produits similaires. Pour mettre en œuvre cette forme de discrimination, les commerçants recourent à des algorithmes de tarification personnalisée (« ATP »), qui s'appuient sur l'intelligence artificielle (« IA ») pour analyser les données des consommateurs et fixer des prix visant à maximiser les profits. Le fait que ces ATP profitent principalement aux vendeurs dans le contexte numérique laisse entrevoir une défail-lance de marché nécessitant une attention particulière, voire une intervention réglementaire. En outre, la discrimination par les prix peut nuire de manière significative au bien-être des consom-mateurs ainsi qu'à la concurrence, notamment lorsque les ATP reposent sur des données biai-sées. Or, à l'heure actuelle, aucune réglementation canadienne n'encadre spécifiquement l'utilisation des ATP ou la discrimination par les prix. L'auteur propose un survol des ATP et recommande la mise en place d'un code de réglementation ex ante, fondé sur des règles claires et inspiré des cadres juridiques en vigueur aux États-Unis et dans l'Union européenne. Ce code viserait notamment à interdire la collecte

et l'utilisation de données personnelles à des fins de ta-rification personnalisée, à imposer des obligations en matière de transparence et de consente-ment éclairé des consommateurs, ainsi qu'à exiger une évaluation continue des ATP. L'objectif est de prévenir les périls liés à la tarification personnalisée dans le marché numérique.

In light of the expanding digital marketplace, more and more consumers are being subjected to price discrimination, whereby consumers are charged different prices for a similar item sold by the same vendor, without their knowledge. To perform price discrimination, sellers (often large companies) implement personalized pricing algorithms ("PPAs"), which use artificial intelligence ("AI") to analyze consumer data to set prices that achieve the maximum amount of profit. PPAs have generated profit for numerous companies; therefore, their popularity and widespread use will likely grow.

The fact that PPAs are benefitting sellers in the digital marketplace suggests that a market failure exists that warrants attention and regulation. Specifically, the extent to which companies can effectively use PPAs is *prima facie* evidence of market power. Without market power, competition amongst sellers would result in consumers diverting their business when the PPA user attempts to charge a high price. Such diversion would defeat any profitability arising from PPA use. Furthermore, companies can use PPAs to facilitate various anti-competitive acts to maintain market power.

While price discrimination can significantly harm consumer welfare and influence market competition, Canada currently has minimal regulations against AI, PPAs and price discrimination. This paper provides an overview of PPAs and suggests the implementation of an *ex-ante*, rules-based regulatory code inspired by international frameworks to prevent the perils of personalized pricing in the digital marketplace.

1. Personalized Pricing Algorithms

The personalized pricing process begins with the collection of "Big Data" - extremely large and diverse data sets that continue to grow at accelerating rates as new information arises.[1] PPAs gather details about the personal characteristics (e.g., age, gender, religion) and shopping behaviour of consumers. PPAs compile information from online browsing and purchase history across various devices (e.g., computers, phones, tablets, smart watches), as well as offline choices via credit card transactions.[2] PPAs then use the collected data to calculate and set prices based on consumers' maximum willingness to pay ("WTP").[3] The result is effectively first-degree

price personalization - a type of price discrimination by which each individual consumer is charged a different price for the same product sold by the same vendor.[4] Since first-degree price personalization requires substantial information about each consumer, it was almost impossible prior to the widespread availability of AI algorithms and broad database of online information.[5] Now, several major retailers use PPAs to set their prices based on consumers' WTP.[6]

2. Potential Harms of Personalized Pricing Algorithms

PPAs pose many risks for consumers in the digital marketplace, especially those belonging to minority groups. Companies and competition may also be adversely affected. Consumers tend to have a negative attitude towards price personalization, which is partially attributed to the secrecy around PPA use.[7] Moreover, consumers often view personalized pricing as unfair, especially if they become aware of price discrepancies that cause them to pay more for a product.[8] In turn, an "unraveling of markets" may occur – if consumers lose confidence that they are receiving a fair price, they may withdraw their demand, leading to fewer sales and lower profits for the company.[9]

2.1 Consumer Welfare and Competition

PPAs may harm consumer welfare since the opacity of pricing algorithms and the broad database of online consumers increase the risk of PPAs producing unfair and supracompetitive prices. One difficulty with AI is the "black box" problem – the inability to comprehend and explain how AI systems arrive at decisions.[10] In the context of PPAs, we know that consumer data is collected and analyzed, but details of the *exact* process by which the data is analyzed remain unclear. Consequently, preventing the generation of unfair prices can be challenging if algorithms function without human intervention.

Additionally, companies rarely, if at all, disclose their collection and use of personal data, so consumers cannot provide consent or prepare for various privacy-related consequences (e.g., data breaches, malware, cybercrimes). PPAs also hinder consumers' ability to make informed purchases by managing their perception of price.[11] In the digital marketplace, consumers cannot see, and are often unaware of, the alternative prices for products offered to other consumers. Sellers can exploit consumers by imposing excessive prices if consumers believe the prices are on-par with the market value of the good or service.[12] Therefore, the use of personal data

in a non-transparent manner strips away the rights of consumers to consent to the use of their data, protect their privacy and make informed decisions.

Companies may also have incentives to implement PPAs in a way that adversely impacts marketplace competition. Global online retailers have been alleged to engage in anti-competitive behaviour and predatory pricing. Such retailers have been said to undercut competitors by using algorithms to track and automatically match or beat their prices, while calculating and pricing items based on consumers' WTP.[13] Some may argue that pricing algorithms maximize competition, by offering lower prices to consumers than they are offered elsewhere. However, certain retailers may use pricing algorithms to extend their monopolies from one market (the online retailing) to a connected market (the online superstore market) by excluding competitors and thereby harming competition.

Companies, such as Postmates, may facilitate joint price-setting by bringing together numerous businesses, which otherwise operate independently. Postmates may allow companies to delegate pricing to a proprietary algorithm, which could set the same excessive prices for similar menu items across different competing restaurants, thus facilitating (either explicit or tacit) collusion. Further, if the algorithm can calculate consumers' WTP, first-degree price personalization can occur.[14]

Additional competition concerns with PPAs include strong network effects, which companies may exploit to maintain dominant positions in the digital marketplace,[15] and the creation of stable cartels from concurrent price discrimination and algorithmic collusion.[16] Given the popularity and effectiveness of PPAs in the digital marketplace, regulation is a reasonable next step to manage market power and prevent the use of PPAs in an anti-competitive manner.

2.2 Bias

One misconception of algorithmic pricing is that a consumer's WTP is derived solely from their preferences.[17] However, AI algorithms are not 100% accurate since they are influenced by bias in the data sets. Bias can be introduced purposefully or inadvertently into AI systems,[18] or implicitly emerge as algorithms operate on data.[19] Therefore, statistical, algorithmic and human cognitive and perceptual biases, such as racism and other forms of discrimination, can influence outputs.[20]

2.2.1 Gender

PPA-generated prices often reflect consumer demographics and may disfavour minorities and disadvantaged groups.[21] In particular, PPAs disproportionately impact women by effectively including a "pink tax" in WTP calculations. A "pink tax" refers to the extra costs women pay for products and services marketed specifically towards them.[22] Although pink taxes typically are found to apply to feminine care products, there is a price discrepancy between sexes in everyday essentials, such as clothes and toiletries. Studies have found that, on average, products that are marketed for women are 13% more expensive than the same products marketed for men.[23] Through their reliance on demographic information, implicit algorithmic bias may emerge - PPAs may assume women have a higher WTP and set their prices at higher rates than men. In light of the pre-existing wage gap, increased prices on products will further disadvantage female consumers.

Gender bias in algorithms can also negatively influences female business owners and employees. A 2016 study found that female vendors on eBay received fewer bids and lower offers than their male counterparts selling the same product.[24] Additionally, the study found that female employees of a ride-sharing company were negatively impacted by the company's algorithm that allocates work and determines compensation rates. Female employees received an average per-hour income of two thirds of male employees, even though they worked more hours.[25] Overall, the use of biased algorithms in the digital marketplace disproportionately harms women by contributing to less compensation, but greater consumer costs.

2.2.2 Race

Similar to gender, data about a consumer's race can influence their calculated WTP since algorithmic bias tends to set higher prices for racial minority groups. For instance, a study performed in 2015 found that the algorithm used by the Princeton Review, a company that provides test preparation, tutoring, and college admissions services for students, was twice as likely to charge higher prices in zip codes with predominantly Asian American populations, irrespective of income.[26] More recently, in 2021, a study analyzing various ride-sharing services found that fares were higher for trips beginning or ending in neighbourhoods with mainly non-white populations.[27] Therefore, while the use of demographic statistics may seem harmless, the inclusion of race in data sets inserts social bias into the analysis and contributes to discriminatory PPA outputs. For individuals with

intersecting minority identities, such as women of colour, the harm is even greater.

2.2.3 Age

A consumer's age can influence their calculated WTP, albeit to a less predictable degree than gender or race. Age is a key characteristic that has historically been used in various marketplaces for third-degree price discrimination, where consumers are charged "differently, for similar products, according to the group they belong to, inferred by attributes of the group."[28] Movie theatres and public transportation, for example, engage in third-degree price discrimination by charging lower prices for youth and seniors. While age discounts benefit these groups of consumers, those whose ages do not fall within the range allocated to youth or seniors will pay higher relative prices. Thus, by using data solely about a consumer's age, rather than their purchase history, PPAs may tend to set higher prices based on inaccurate assumptions about consumers' WTP. Such assumptions can be harmful – considering a person's earnings are not directly correlated with their age, a consumer may be subjected to higher prices without having the proportional economic means to afford them.

3. Current Regulations

3.1 AI Legislation

Despite being at the forefront of AI,[29] Canada currently has no regulatory framework specific to PPAs or price discrimination. In June of 2022, the *Artificial Intelligence and Data Act* (the "*AIDA*") was introduced in Parliament as part of Bill C-27 to address the adverse impacts of AI on individuals and in the commercial context.[30] The *AIDA* established regulatory standards for "high-impact" AI systems around safety and human rights and creates new criminal law provisions to prohibit harmful uses of AI.[31] Regulatory requirements included human oversight and monitoring, transparency in data collection and use, and the proactive assessment of high-impact AI systems to identify likely harms, accountability and consistency in outputs. Violations of the *AIDA* would result in administrative monetary penalties ("AMPs"), regulatory offences and criminal offences.[32] However, Bill C-27, and thus the *AIDA,* was terminated due to the prorogation of Parliament on January 6, 2025.

AI use in the private sector is mainly regulated by the Voluntary Code of Conduct on the Responsible Development and Management of Advanced Generative AI Systems. The Code provides Canadian companies with

common standards regarding safety, fairness, transparency, etc., and allows them to demonstrate that they are developing and using generative AI systems in a responsible manner.[33] For instance, the Code requires developers to assess training data sets to manage data quality and potential biases, as well as perform various testing to assess and mitigate the risk of biased output prior to release.[34] So far, major firms have signed the Code, such as Cohere, Ada, Coveo, BlackBerry, TELUS, OpenText, and IBM.[35]

3.2 The *Competition Act*

Without AI-specific legislation, Canada's *Competition Act*[36] may be used to address the harms associated with PPAs. While no provision specifically prohibits price personalization or price discrimination generally,[37] subsection 78(1)(k) lists the imposition of excessive and unfair selling prices as one of the definitions of "anti-competitive acts" for the purposes of section 79, which concerns abuse of dominance.[38] PPA use may be considered anti-competitive under subsection 78(1)(k) or under section 78(1) more generally if framed as predatory, exclusionary or disciplinary when used to target competitors.[39] However, subsection 78(1) states that "anti-competitive acts" must be intended to negatively affect a competitor or market competition, or substantially harm competition in effect. In light of the black box nature of AI, malicious intent and anti-competitive effects may be difficult to establish. Users may argue that they were unaware of the potential for their PPAs to influence competition, and tracing specific anti-competitive effects to a single algorithm is, at present, almost impossible. As a result, there is currently a lack of evidence that PPAs cause substantial harm to competition, which is also problematic for subsection 79(1)(b)(i), which prohibits conduct that had, is having, or is likely to have the effect of preventing or lessening competition. Furthermore, the Competition Bureau expects that claims of excessive and unfair pricing will be rare as investigations require a credible reason to suspect the occurrence of anti-competitive acts or substantial competition harm.[40]

The *Competition Act* also includes provisions which address misleading representations and deceptive marketing practices. Section 52 and subsection 74.01(1)(a) prohibit companies from making materially false or misleading representations to promote a product, service or business interest.[41] While these provisions only explicitly refer to positive representations, omissions may be captured by the "general impression test" used by courts when deciding whether a representation is false or misleading. The general impression test requires courts to consider the general impression conveyed by the representation as well as its literal meaning.[42] Since companies rarely,

if ever, disclose their use of PPAs, these provisions will likely not capture such acts. There is also no guarantee that a court will find that failure to disclose a PPA constitutes a false or misleading representation under the general impression test. In turn, a possible amendment to section 52 and subsection 74.01(1)(a) to enhance their effectiveness at regulating PPAs is to explicitly prohibit omissions.

Additionally, sections 45 or 90.1 may be applicable if an agreement or arrangement exists amongst competitors to use PPAs to lessen competition in the digital marketplace.[43] Nevertheless, since algorithmic tacit collusion is more common than explicit collusion and with the minimal explainability of PPAs, demonstrating that pricing algorithms coordinated their actions and engaged in collusive behaviours to produce supracompetitive pricing or reduce competition is no easy feat and not adequately regulated with *ex-post* measures.[44]

Considering the difficulty with tracing harm to competitors and market competition to a particular pricing algorithm, no statutes or cases currently address the legality of PPAs. In fact, a case law search on the Competition Bureau website produces no results. Therefore, other than industry-specific regulations and consumer protection statutory provisions, prices are largely unregulated and left to the contracting parties.[45]

3.3 The United States

3.3.1 AI Legislation

Currently, the United States does not have any comprehensive federal legislation to regulate AI. However, the *Algorithmic Accountability Act of 2023* (the "*AAA*") was proposed in Senate to regulate AI in "high-impact" scenarios, such as housing, finance, employment and education,[46] where algorithms decide loan approvals, medical needs, hiring outcomes of new employees, school admissions, etc. The *AAA* aims to promote greater transparency about the impact of algorithms by requiring users to conduct impact assessments for effectiveness, bias and other factors, as well as perform ongoing testing to ensure outputs are accurate and do not amplify bias based on personal characteristics.[47] In addition, the *AAA* proposes that the Federal Trade Commission (the "FTC") establish a Bureau of Technology to monitor the enforcement and implementation of the Act. At the state level, Colorado, Utah, Illinois, Massachusetts, Ohio and California have all proposed or enacted legislation to regulate AI development and use in the private sector.[48] Most state legislation focuses on similar high-impact situations as the *AAA* and the safe development of AI models. Unfortunately,

PPAs are rarely, if at all, used in these high-impact scenarios, and thus fall outside the ambits of the *AAA* and state legislation.

3.3.2 Privacy Laws

In the US, data privacy laws are the primary form of pricing algorithm regulation. US privacy laws comprise an *ex-post*, sector-based framework that aims to protect the welfare of online consumers.[49] The *Federal Trade Commission Act* (the "*FTC Act*") regulates algorithmic pricing to prohibit deceptive or unfair behaviour or practices. Under section 5 of the *FTC Act,* FTC authority can pursue legal action against someone if their use of an algorithm is deceptive or unfair and causes substantial harm that a) consumers cannot reasonably avoid, and b) is not outweighed by countervailing benefits to consumers or competition.[50] Deceptive use includes a failure to disclose how prices are determined, whereas unfair use involves discriminatory pricing that could harm consumers. For instance, if an online retailer employs a pricing algorithm that discriminates against a consumer by charging them higher prices based on their zip code without disclosing the fact, the retailer will violate the *FTC Act.*

In the context of PPAs, US privacy laws do not effectively mitigate the harms of personalized pricing. First, requiring algorithms to cause substantial consumer harm poses a challenge for PPAs. Given their opacity and use of a plethora of personal information, quantifying and directly attributing consumer harm to a PPA's use of specific data is quite difficult.[51] Consequently, the *FTC Act* may fail to capture many instances of excessive personalized pricing. Second, the decentralized approach to privacy laws allows each state to fill any regulatory voids with their own legislation. For instance, California's *Consumer Privacy Act* and Virginia's *Consumer Data Protection Act* regulate the processing and control of personal data.[52] While state legislation attempts to supplement the *FTC Act* to create comprehensive regulation across the country, the fragmented framework provides uneven protections for consumers - regardless of which state a seller is located in, consumers are only protected by the laws of the state in which they reside. In addition, increased operational complexity and costs arise for businesses that operate in various states since they must comply with the legislative requirements specific to each state. Considering companies in the digital marketplace, such as eBay, span across numerous states and countries, the US privacy law framework does not sufficiently address the harms of PPAs.

3.4 The European Union

To protect consumers from price discrimination created by PPAs, the European Union uses an omnibus approach that involves AI regulation, anti-discrimination laws and data protection legislation.

3.4.1 AI Regulation

In 2024, the EU approved the first risk-based framework for AI – the *Artificial Intelligence Act* (the "*AI Act*").[53] The *AI Act* introduces unique regulations for certain uses of online algorithmic pricing, so AI users in different sectors have varying transparency, data governance and human oversight obligations.[54] Regarding price discrimination, Article 5(1)(c) prohibits the use of AI scoring techniques based on personal characteristics in circumstances where 1) the information is used outside of the context for which it was generated, and/or 2) the detrimental effects are disproportionate to the behaviour.[55] Article 5(1)(c) may capture PPAs since the algorithms analyze personal data provided by consumers in other instances or obtained without consumer knowledge. Furthermore, excessive prices may harm consumers at a rate disproportionate to any consumer or seller benefits. Nonetheless, PPAs may benefit consumers by offering more equitable pricing based on characteristics, such as zip codes, so establishing disproportionate detrimental effects of PPAs is difficult.

3.4.2 Anti-Discrimination Laws

In principle, personalized pricing is legal in the EU, as long as sellers do not use the personal information of consumers in a manner that breaches anti-discrimination laws.[56] Article 21 of the Charter of Fundamental Rights prohibits "discrimination on such grounds as sex, race, colour, ethnic or social origin, genetic features, language, religion or belief, political or any other opinion, membership of a national minority, property, birth, disability, age or sexual orientation."[57] Under Directive 2000/43/EC, discrimination based on grounds of racial or ethnic origin in relation to the supply of goods and services is prohibited.[58] Additionally, Directive 2004/113/EC disallows discrimination on the grounds of sex, such that men and women must receive equal treatment in accessing and supplying goods and services.[59] EU anti-discrimination laws apply to PPAs and prohibit direct and indirect discrimination. A pricing decision based on one of the prohibited grounds is considered directly discriminatory, whereas indirect discrimination occurs if the pricing "has a disproportionate impact on certain groups defined by a prohibited ground without an objective and appropriate justification."[60] If a PPA solely analyzes information about the sex of consumers, pricing

outcomes would differ directly based on sex, one of the prohibited grounds, and thus violate Directive 2004/113/EC. However, since PPAs often use a vast array of personal data to arrive at pricing decisions, indirect discrimination is more likely. If PPAs consider women to have a higher WTP by including "pink tax" in their calculations, the criteria for indirect discrimination can be met.

3.4.3 Data Protection Legislation

3.4.3.1 General Data Protection Regulation

The General Data Protection Regulation (the "GDPR") regulates the treatment of personal data, pseudonymous data and anonymous data originating in the EU,[61] and applies to operations within and outside the EU, including Canada.[62] The GDPR defines personal data as data that directly or indirectly identifies a person, "in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the[ir] physical, physiological, genetic, mental, economic, cultural or social identity."[63] PPAs collect and analyze data about age, sex, religious beliefs, location, etc., which fall under the "personal data" definition. Therefore, users must abide by the GDPR's *ex-ante* and *ex-post* regulations.

Ex-ante measures aim to ensure transparency, accountability and fairness in the use of personal data. For PPAs, relevant requirements include obtaining consumer consent before including their personal data in an algorithmic data set and conducting mandatory Data Protection Impact Assessments ("DPIAs"). Article 9(1) requires consent for the processing of "sensitive" data, such as "personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership."[64] Article 35 mandates DPIAs for various operations, including complex algorithmic pricing schemes.[65] DPIAs require companies to describe how the personal data will be processed and the risks to the rights and freedoms of the individuals, as well as identify measures to address any potential privacy risks.[66] A company must examine how their PPA uses personal characteristics and past purchasing behavioural data to determine pricing, and whether these practices could result in discrimination or unfair treatment.[67] However, given the lack of explainability of AI, companies may struggle to meet the requirement.

Articles 14, 15, 21 and 22 of the GDPR outline the *ex-post* measures applicable to PPAs. Once personal data is collected, Article 14 requires users to explain their algorithms and AI methods to increase transparency[68] – again,

such an explanation may be difficult, if not impossible. Article 15 allows consumers to review the data being analyzed by the PPA,[69] after which they can decide if they want to proceed as a customer of the company. Article 21 provides consumers with the right to object to the processing of their personal data, including profiling.[70] Finally, under Article 22, consumers have the right to challenge decisions solely based on automated processing "which produces legal effects concerning [the consumer] or similarly significantly affects [them]."[71] However, sellers can bypass the provision by involving humans in a minor way, so decisions are not made by "solely automated processing" systems.[72] Furthermore, what constitutes a significant impact on consumers is unclear, so whether the effects of PPAs would fall under the provision remains uncertain.

3.4.3.2 Additional Measures

To supplement the GDPR, the EU implemented the *Digital Services Act* (the "*DSA*") and *Digital Market Act* (the "*DMA*"), which focus on risk and crisis management and fostering a competitive market, respectively. Under the *DSA*, companies who use digital services, including pricing algorithms, must manage online risks and crises effectively to prevent harming consumer rights or public safety.[73] The *DMA* provides objective criteria to qualify large online platforms as "gatekeepers" and establishes clear obligations that gatekeepers must follow to protect consumers from exploitative pricing algorithms. So far, companies such as Amazon, Apple and Microsoft have been designated as gatekeepers.[74]

The Consumer Rights Directive (the "CRD") addressed personalized pricing for the first time in EU legislation. Article 6(1)(ea) of the CRD requires traders to inform consumers if prices are personalized based on automated decision-making.[75] However, the provision does not require disclosure of how prices are calculated (e.g., with an algorithm, based on personal characteristics, etc.), so many instances of personal pricing escape regulation. To overcome the CRD's limited scope, Article 7(1) of the Unfair Commercial Practices Directive imposes a positive obligation on traders to provide all the information necessary for the average consumer to make an informed purchasing decision.[76] For PPAs, "necessary" information could include PPA use and the characteristics being analyzed.

3.5 Learning From the US and EU

When comparing the US and EU approaches to algorithmic pricing, the EU framework provides greater consumer protection.[77] The state-specific and sector-based legislation in the US leads to inconsistent, and often

inadequate, regulation of algorithmic pricing that complicates compliance efforts for companies involved in numerous industries. In comparison, the GDPR provides comprehensive guidelines to promote transparency around PPA use across the EU in various sectors. Additionally, the scope of the language used in each framework has important implications for PPA regulation. The GDPR broadly defines "personal data" to encompass any organization that processes personal data.[78] Such a wide definition creates uncertainty and compliance difficulties for businesses, enforcement issues for regulators and struggles to exercise data rights for individuals.[79] By using the GDPR's definition of personal data, the *DSA* and *DMA* suffer from the same semantic uncertainty. Consequently, future algorithmic pricing legislation should apply a narrower definition that explicitly references the types of prohibited data and uses. Overall, the US and EU frameworks highlight how PPAs require comprehensive regulation that applies to all sectors, contains precisely defined terms, incorporates *ex-ante* disclosure and consumer consent requirements and mandates ongoing monitoring to ensure compliance as AI algorithms evolve.

4. Proposed Reform

Canada should implement a licensing regime for e-commerce sellers based on a code (the "Code") that includes *ex-ante*, rules-based requirements, ongoing measures and AMPs for violations. With the growing availability of online personal data and the development of more intricate algorithms, personalized pricing will be increasingly easy to perform.[80] Considering the limitations of current *ex-post* regimes, namely the *Competition Act,* PPAs should be regulated in an *ex-ante* manner to prevent certain personal data from entering algorithms, generating implicit data bias and producing unfair, excessive prices, especially for consumers belonging to minority groups who face societal and financial disadvantages. While some individuals advocate for a blanket ban on personalized pricing, experts warn that a full prohibition could harm disadvantaged consumers who may benefit from fair and responsible personalized pricing.[81] For instance, if a PPA detects a consumer is located in a lower-income neighbourhood, the algorithm may generate a lower price.

4.1 Regulatory Framework

Purpose

(1) This Code aims to reduce the potential and actual harms to consumers and market functioning associated with first-degree price personalization

arising from the use of personalized pricing algorithms in the digital marketplace.

Definitions

(2) In this Code,

"First-degree price personalization" means the practice of pricing the same product or service from the same seller at a different rate for each individual consumer.

"Personal data" means information that directly or indirectly refers to an individual's physical, physiological, genetic, mental, economic, cultural or social identity. Such information includes sex, gender, age, religion, race, national or ethnic origin, name, occupation, social security number, phone number, email address, credit card information and transactions, zip code, IP address, device ID, MAC address, cookies and browser fingerprints.

"Personalized pricing algorithms ('PPAs')" means algorithms that use artificial intelligence to generate the price of a product or service for a consumer according to calculations of that consumer's willingness to pay based on their personal data.

"Seller" means any individual person or company that uses a PPA to sell, or coordinate the sale of, a good or service in the digital marketplace.

"Willingness to pay ('WTP')" means the maximum amount a consumer is willing to spend to purchase a good or service.

Application

(3) This Code applies to PPAs developed and used for all e-commerce transactions, across all industries and sectors, where the seller and/or consumer is located in Canada.

Licence Issuance

(4) A regulatory authority may issue a licence to a seller to use a PPA to price online goods and services if the algorithm and seller act in accordance with the rules and requirements provided in sections 5 and 6 of this Code, respectively.

Prohibited Activities

(5) A seller shall not implement a PPA to generate the price of goods and services based on any characteristic(s) considered "personal data" under section 2 of this Code. Some rules include:

a) PPAs shall not price men's products and women's products sold by the same seller, of the same nature, quality and material, at a higher rate than the other. Product labels including the words "girl," "boy," "female," "male," "women," and/or "men" must be excluded from the PPA data sets.

b) PPAs shall not charge a consumer with an IP address associated with a higher-income neighbourhood (annual household income of over $150,000) a higher price for goods and services than a consumer with an IP address associated with a middle-income (annual household income between $65,000 to 150,000) or lower-income area (annual household income under $65,000).

c) PPAs shall not analyze information about a consumer's sex or gender, obtained from direct or indirect identifiers, to calculate that consumer's WTP. Identifiers of sex and gender include the consumer's name, pronouns and gender labels on previously purchased products.

Disclosure and Consent Requirements

(6) Sellers must disclose their use of PPAs to consumers at the first instance that consumers access the seller's e-commerce platform. Sellers must disclose that the prices on the platform are personalized and calculated with a PPA using the personal data of each individual consumer. This disclosure must include an option for consumers to consent to the terms of disclosure and proceed to the platform or withhold consent and be redirected off the platform.

Ongoing Measures

(7) After receiving a licence, a seller must:

a) Outline a schedule for performing four (4) internal audits per year to assess for bias and any personal characteristics outlined in section 2 of this Code in the algorithmic data sets;

b) Perform a risk assessment and prepare a report detailing their incident response plan to any risks identified in the assessment; and

c) Establish a specific team and/or individual (e.g., a Model Risk Officer) to oversee the routine audits and data management.

Violations

(8) Failure to abide by any measure(s) in sections 5, 6 and/or 7 constitutes a violation of this Code. A seller who commits a violation shall have their licence revoked by the authority and is liable

a) in the case of an individual seller, to a maximum administrative monetary penalty of $50,000; or

b) in the case of a company, to a maximum administrative monetary penalty of $5,000,000.

Criteria for Penalty

(8.1) The amount of the penalty is to be determined by considering factors such as:

a) the nature and extent of the violation;

b) any benefit obtained by the seller from committing the violation;

c) the seller's ability to pay the penalty; and

d) any other factor considered relevant by the seller or authority.[82]

4.2 Rationale for a Rules-Based Approach

Rules clearly outline what conduct is prohibited, thus reducing subjectivity and increasing the efficiency of the licensing process.[83] A rules-based system is arguably better suited for actions that are "simple, stable and do not involve huge economic interests."[84] Nevertheless, while AI algorithms are complex, dynamic and may generate prices for substantial e-commerce purchases, a rules-based code with explicit instructions can effectively regulate unfair price personalization. Although AI is rapidly evolving, the information targeted by the Code is often simple and stable since personal characteristics (e.g., gender, race, religion) are unlikely to change significantly over time.

A rules-based code also increases the efficiency of the licensing process. *Ex-ante* regulations are critiqued as being inefficient since regulators must review each product.[85] However, rules contribute to a more efficient approval process by requiring objective determinations, rather than

subjective assessments under principles-based legislation - whether an algorithm uses prohibited data can be better determined than whether an algorithm generates "unfair" prices. Rules also reduce the likelihood of interpretation issues. A principles-based code prohibiting "unfair" pricing is unclear - one seller might consider charging consumers in a wealthy neighbourhood a higher price as fair, while another may not. The former seller may be denied a licence if the regulator decides their algorithm generates unfair prices, creating a delay as the seller must amend their algorithm and reapply. Additionally, rules promote consistency. What one regulator considers "unfair" differs from the next, so empowering regulators to determine what constitutes "unfair" pricing results in inconsistent approvals and an unjust advantage for sellers who have their PPAs assessed by a more lenient regulator. Clear and objective rules limit discretion and ensure that decisions align with the Code's purpose.

4.3 Rationale for an *Ex-Ante* Framework

Ex-ante measures require the proactive integration of safeguards to protect consumers, rather than a reaction to harm that has already occurred. According to the Ontario Court of Appeal, "there is good reason to favour *ex-ante* rules where … there is scientific uncertainty as to the precise nature or magnitude of the possible harms."[86] Given the automatic functioning of PPAs and lack of, or minimal, human involvement, uncertainty exists around the precise magnitude of harmful pricing that occurs. Furthermore, *ex-ante* regulation may be beneficial in circumstances that involve "invisible harms" - harms that go unreported because they are difficult or impossible to identify by design or due to a lack of will or mechanism to report.[87] Considering the opacity of PPAs, bias from past discrimination based on personal characteristics may enter the algorithm and contribute to perilous price personalization without being detected and/or reported. Consequently, PPAs create invisible harms that could be prevented with *ex-ante* regulation. Finally, an *ex-ante* code would complement the *Competition Act* and enhance its efficacy in regulating PPAs. Since section 6 of the Code requires disclosure of PPA use, failure to provide accurate and adequate information may trigger section 52 and subsection 74.01(1)(a), the false and misleading representation provisions, and reduce reliance on the general impression test.

4.3.1 Response to Potential Objections

According to Archibald & Jull, *ex-ante* regulation should be reserved for situations where health and safety are at risk, but do not have to be

life-threatening.[88] While PPAs do not directly influence consumer health and safety, the downstream effects of harmful personalized pricing may be exceptionally harmful to consumer welfare. A consumer may rely on a product and become accustomed to a certain price. If a PPA calculates a higher WTP for that consumer, the price may increase and force the consumer to choose to access the product or pay an excessively high price.[89] Furthermore, health and personal care is the second fastest growing e-commerce industry,[90] contributing over $4.9 billion CAD in revenue in 2024. Consumers purchase health-related products online; therefore, restricted access because of extreme prices could harm consumer health. Moreover, the privacy and security of personal data has implications for consumer safety. As Peter Seele et al. explain, "online and offline tracking, profiling, and personalizing is becoming ubiquitous, leaving less and less room for consumers' privacy."[91] Since sellers often mask their use of personal data with extensive privacy disclaimers, many consumers are unaware of such processes and thus unable to take the necessary measures to protect their data against situations like data breaches.

An indirect connection to health and safety may be rejected as a valid basis for *ex-ante* regulation. However, *ex-ante* legislation should not be dismissed as one could argue the Archibald & Jull model is too restrictive. As discussed, principled reasons exist for *ex-ante* PPA regulation, such as the fact that initially preventing bias and personal characteristics from entering data sets will most effectively prevent unfair prices. As a result, there ought to be a role for *ex-ante* frameworks even where health and safety are not directly impacted. The biggest obstacle to acceptance is that *ex-ante* systems are inflexible and considered inappropriate for situations where technology is rapidly developing since "prior approval may lag behind the technological progress."[92] In such circumstances, *ex-post* regulation, such as the *Competition Act* provisions concerning excessive pricing[93] and consumer protection,[94] are traditionally viewed as more fitting, if anti-competitive effects can be demonstrated. With AI quickly evolving, PPA users often update their pricing algorithm models to enhance data learning and predictive capabilities over time. However, the Code does not target these developments, but rather focuses on the *type* of data being analyzed by outlining rules that algorithms must follow, regardless of their model. Since each PPA version analyzes the same data and approval depends on the type of data being analyzed (e.g., personal characteristics), technological advancements in their algorithm's efficiency at collecting and analyzing data will not impact prior approval.

Considering the Code's novelty and stringency, resistance is expected. First, the government will be hesitant to implement the *ex-ante* Code since the licensing process requires significant monetary and temporal resources. A tradeoff exists – while it is more time efficient to conduct *ex-post* reviews of evidence of anti-competitive conduct and address it accordingly, significant harm may go undetected and unaddressed due to the lack of algorithmic explainability. Reviewing individual algorithms will certainly take time since sellers may not use the exact same algorithms as one another; nonetheless, pricing algorithms use similar foundations, variables, weighting and decision rules.[95] Therefore, the review process may be less time consuming than initially believed and sellers may obtain licences in a timely fashion. Second, e-commerce sellers will likely oppose the Code because the approval of their algorithms lies in the hands of government officials with whom they may disagree and there may be a discrepancy in the quality and attentiveness of regulators. However, the Code's objective rules may ease some concerns by reducing the subjectivity of the decision-making process and promoting consistency across licencing decisions.

Overall, the Code provides sufficient safeguards against the inflexibility and potential objections to warrant an *ex-ante* regulatory framework for PPAs. At the end of the day, the victims of unfair price personalization are the consumers. With over 75% of the Canadian population being e-commerce users,[96] the likelihood of biased price discrimination is not insignificant, and may cause detrimental harm over time if consumers, especially those belonging to minority groups, are charged supracompetitive prices for goods and services.

4.4 Ongoing Measures

Ongoing measures are crucial to promote compliance and identify prices based on bias or personal data, as well as address the evolving nature of PPAs. Quarterly audits are an effective accountability, bias and general risk mitigation mechanism.[97] Given the rapid development of AI, audits allow users to identify and remove any bias or prohibited information that may have entered the data sets to mitigate unfair pricing outputs. Furthermore, risk assessments allow for proactively planning to address anti-competitive risks that may materialize during PPA use, enabling companies to complete their due diligence. Finally, having a delegated team or officer aids in monitoring compliance and reporting potential violations.[98]

4.5 Penalties

AMPs will encourage compliance and prevent violations of the licensing requirements. The penalty scheme takes inspiration from other *ex-ante* legislation in Canada,[99] accounting for the severity of the violation and the resulting harm. When administering AMPs, there is a risk that the penalties will be considered a true penal consequence and trigger *Charter* rights. In *Guindon v Canada,* the Supreme Court of Canada (the "SCC") found that a monetary penalty will be a true penal consequence "when it is, in purpose or effect, punitive."[100] To determine whether an AMP is punitive and thus inappropriate in a regulatory context, the SCC outlined four factors that should be balanced – "the magnitude of the fine, to whom it is paid, whether its magnitude is determined by regulatory considerations rather than principles of criminal sentencing, and whether stigma is associated with the penalty."[101]

Based on the *Guindon* factors, the Code's penalty scheme does not produce true penal consequences. While $50,000 and $5,000,000 may seem significantly high and punitive in nature, the size of most PPA users (e.g., eBay) and the reach of the algorithms (one PPA can target every consumer and impact millions of people) is substantial and warrants a high penalty. It should also be noted that these values represent the maximum AMP amounts under the scheme and, therefore, will not necessarily be administered for each violation. Moreover, the amounts are directly tied to the objective of deterring non-compliance with the Code and account for the reality that many consumers purchase most of their daily necessities online, so excessive prices can be detrimental to their livelihoods. An authority must also consider various factors in determining the magnitude of the AMP (such as the violator's personal gain), which are relevant to deterring such misconduct. Finally, the stigma arising from the imposition of an AMP under the Code is not comparable to that attached to a criminal conviction, but rather is similar to the penalties for other regulatory offences, such as violations of the *Occupational Health and Safety Act.*[102]

5. Conclusion

With the rapid expansion of the digital marketplace, the use of PPAs is bound to increase and influence a greater number of consumers. Despite *prima facie* evidence of market power of effective PPA users, as well as the significant risks of excessive prices, especially for minority groups, and anti-competitive behaviour, Canada currently lacks an adequate regulatory scheme for PPAs. Taking inspiration from the US and EU regulatory

frameworks, Canada should implement a licensing regime based on an *ex-ante,* rules-based code with ongoing measures and AMPs to reduce the perils of personalized pricing in the digital marketplace.

ENDNOTES

* Tristan Montag is a JD candidate at University of Toronto Faculty of Law. I would like to thank Kenneth Jull for his invaluable guidance, Suzana Popovic-Montag for her unwavering support, and the editors at the CCLR who provided feedback on the article.

1 Amanpreet K Sandhu, "Big Data with Cloud Computing: Discussions and Challenges" (2022) 5:1 Big Data & Mining Analytics 32 at 33.

2 Thomas Mattes, "Algorithmic Price Administration: How Amazon Hijacks the Price System" (2022) 37:4 BTLJ 1489 at 1500–01.

3 Pascale Chapdelaine, "Algorithmic Personalized Pricing: A Personal Data Protection and Consumer Law Perspective" (2024) 102:1 Can Bar Rev 1 at 3.

4 Aymeric de Moncuit et al, "AI Challenges in Competition Law – How Are Regulators Responding?" *PLC Magazine* (April 2024), online: <mayerbrown.com/-/media/files/perspectives-events/publications/2024/04/ai-challenges-in-competition-law_mar24.pdf%3Frev=55168f8e10a64e458c3fc1ac7af179df>.

5 Axel Gautier, Ashwin Ittoo & Pieter Van Cleynenbreugel, "AI algorithms, price discrimination and collusion: a technological, economic and legal perspective" (2020) 50 Eur J L & Econ 405 at 409.

6 Salil K Mehra, "Price Discrimination-Driven Algorithmic Collusion: Platforms for Durable Cartels" (2021) 26:1 Stan JL Bus & Fin 171 at 171, 185.

7 Peter Rott, Joanna Strycharz & Frank Alleweldt, *Personalised Pricing* (Luxembourg: Policy Department for Economic, Scientific and Quality of Life Policies, 2022) at 6.

8 Paolo Pautassi, *Algorithmic Pricing in the digital age* (Masters Dissertation, Politecnico di Torino, 2024) [unpublished] at 39.

9 Competition & Markets Authority, "Pricing algorithms" (2018) Working Paper No 94, online: <assets.publishing.service.gov.uk/media/5bbb2384ed915d238f9cc2e7/Algorithms_econ_report.pdf> at 50.

10 Manuel Carabantes, "Black-box artificial intelligence: an epistemological and critical analysis" (2020) 35 AI & Soc 309 at 309.

11 Mattes, *supra* note 2 at 1503.

12 Qian Li, Niels Philipsen & Caroline Cauffman, "AI-enabled price discrimination as an abuse of dominance: a law and economics analysis" (2023) 9 China-EU LJ 51 at 64.

13 Mattes, *supra* note 2 at 1509.

14 Mehra, *supra* note 6 at 187.

15 See Competition & Markets Authority, *supra* note 9 at 49.

16 See Mehra, *supra* note 6.

17 Oren Bar-Gill, "Algorithmic Price Discrimination When Demand Is a Function of Both Preferences and (Mis)perceptions" (2006) 86:2 U Chicago L Rev 33.

18 Reva Schwartz et al, *Towards a Standard for Identifying and Managing Bias in Artificial Intelligence* (Washinton: National Institute of Standards and Technology, 2022) at 3.

[19] Gabbrielle M Johnson, "Algorithmic bias: on the implicit biases of social technology" (2020) 198 Synthese 9941.
[20] Schwartz et al, *supra* note 18 at 9–10.
[21] Peter Seele et al, "Mapping the Ethicality of Algorithmic Pricing: A Review of Dynamic and Personalized Pricing" (2021) 170 J Bus Ethics 679 at 712.
[22] Kelley R Taylor, "Pink Tax: What Does Price Discrimination Cost Women?" (last modified 6 September 2024), online: <kiplinger.com/taxes/pink-tax-womens-products-price-discrimination>.
[23] Bill de Blasio & Julie Menin, *From Cradle to Cane: The Cost of Being a Female Consumer* (New York City: Department of Consumer Affairs, 2015).
[24] Galit P Wellner, "When AI is Gender-biased: The Effects of Biased AI on the Everyday Experiences of Women" (2020) 13:37 J Phil Stud 127 at 130.
[25] *Ibid.*
[26] Keyon Vafa et al, "Price Discrimination in The Princeton Review's Online SAT Tutoring Service" (2015) Tech Sci at 8.
[27] Akshat Pandey & Aylin Caliskan, "Disparate Impact of Artificial Intelligence Bias in Ridehailing Economy's Price Discrimination Algorithms" (Paper delivered at the 2021 AAAI/ACM Conference on AI, Ethics, and Society, 30 July 2021), online: <dl.acm.org/doi/10.1145/3461702.3462561>.
[28] Ana CB Garcia, Marcio GP Garcia & Roberto Rigobon, "Algorithmic discrimination in the credit domain: what do we know about it?" (2024) 39 AI & Soc 2059 at 2061.
[29] Government of Canada, "Securing Canada's AI Advantage" (7 April 2024), online: <pm.gc.ca/en/news/news-releases/2024/04/07/securing-canadas-ai>.
[30] Government of Canada, "The Artificial Intelligence and Data Act (AIDA)—Companion Document" (modified 13 March 2023), online: <ised-isde.canada.ca/site/innovation-better-canada/en/artificial-intelligence-and-data-act-aida-companion-document>.
[31] *Ibid.*
[32] *Ibid.*
[33] Government of Canada, "Voluntary Code of Conduct on the Responsible Development and Management of Advanced Generative AI Systems" (September 2023), online: <ised-isde.canada.ca/site/ised/en/voluntary-code-conduct-responsible-development-and-management-advanced-generative-ai-systems>.
[34] Government of Canada, "Companion Document", *supra* note 30.
[35] Government of Canada, "Canada's AI Advantage", *supra* note 29.
[36] *Competition Act*, RSC 1985, c C-34.
[37] Mehra, *supra* note 6 at 204.
[38] *Competition Act*, *supra* note 36, ss 78(1)(k), 79.
[39] *Ibid*, s 78(1).
[40] Competition Bureau Canada, "Changes to the Provisions on Mergers and Restrictive Trade Practices in the Competition Act" (7 November 2024), online: <competition-bureau.canada.ca/en/mergers-and-acquisitions/changes-provisions-mergers-and-restrictive-trade-practices-competition-act>.
[41] *Competition Act*, *supra* note 36, ss 52, 74.01(1)(a).

[42] Competition Bureau Canada, "The general impression test" (22 November 2024), online: <competition-bureau.canada.ca/en/deceptive-marketing-practices/general-impression-test>.
[43] *Competition Act*, *supra* note 36, ss 45, 90.1.
[44] Mehra, *supra* note 6 at 187.
[45] Joshua Karton, "Piecemeal Solutions to Demonstrated Problems of Unfairness: Control of Price Terms in Common Law Canada" in Yesim M Atamer & Pascal Pichonnaz, eds, *Control of Price Related Terms in Standard Form Contracts* (Basel: Springer International Publishing, 2019).
[46] US, Bill S 2892, *Algorithmic Accountability Act of 2023*, 118th Cong, 2023.
[47] *Ibid*.
[48] Julie Himo et al, "What's new with artificial intelligence regulation in Canada and abroad?" (last visited 10 November 2024), online (blog): <torys.com/en/our-latest-thinking/resources/forging-your-ai-path/artificial-intelligence-regulation-in-canada-and-abroad>.
[49] Zihao Li, "Regulating Online Algorithmic Pricing: A Comparative Study of Privacy and Data Protection Laws in the EU and US" (2024) Stanford Law School and the University of Vienna School of Law, Working Paper No 114 at 19.
[50] Emmanuel Pernot-Leplay, "China's Approach on Data Privacy Law: A Third Way Between the US and the EU?" (2020) 8:1 Penn St J L & Intl Aff 51 at 55–62.
[51] Li, *supra* note 49 at 21.
[52] *Ibid* at 20.
[53] Steven Farmer, Scott Morton & Mark Booth, "The EU's AI Act: A Review of the World's First Comprehensive Law on Artificial Intelligence and What This Means for EU and Non-EU Companies" (19 July 2024), online: <pillsburylaw.com/en/news-and-insights/eu-ai-act.html>.
[54] Li, *supra* note 49 at 31.
[55] Future of Life Institute, "The AI Act Explorer" (last visited 17 October 2024), online: <artificialintelligenceact.eu/ai-act-explorer/>.
[56] Rott, Strycharz & Alleweldt, *supra* note 7 at 7.
[57] *Ibid* at 24.
[58] *Ibid*.
[59] *Ibid*.
[60] Laura Drechsler & Juan CB Sánchez, "The Price is (Not) Right: Data Protection and Discrimination in the Age of Pricing Algorithms" (2018) 9:3 Eur J L & Tech 1 at 5.
[61] Paul Voigt & Axel von dem Bussche, *The EU General Data Protection Regulation (GDPR): A Practical Guide* (Cham: Springer International Publishing, 2017).
[62] 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 [GDPR].
[63] *Ibid*, art 4(1).
[64] *Ibid*, art 9(1).

[65] *Ibid*, art 35.
[66] *Ibid*.
[67] Li, *supra* note 49 at 11–12.
[68] GDPR, *supra* note 62, art 14.
[69] *Ibid*, art 15.
[70] *Ibid*, art 21.
[71] *Ibid*, art 22.
[72] Li, *supra* note 49 at 18.
[73] *Ibid* at 31.
[74] European Commission, "The Digital Markets Act: ensuring fair and open digital markets" (last visited 30 November 2024), online: <commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/digital-markets-act-ensuring-fair-and-open-digital-markets_en>.
[75] EU, *Directive 2011/83/EU of the European Parliament and of the Council of 25 October 2011 on consumer rights, amending Council Directive 93/13/EEC and Directive 1999/44/EC of the European Parliament and of the Council and repealing Council Directive 85/577/EEC and Directive 97/7/EC of the European Parliament and of the Council*, [2011] OJ L 304/64, art 6(1)(ea).
[76] EU, *Directive 2005/29/EC of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market*, [2005] OJ L149/22, art 7(1).
[77] Li, *supra* note 49 at 26.
[78] Nadezhda Purtova, "The Law of Everything: Broad Concept of Personal Data and Future of EU Data Protection Law" (2018) 10 L Innovation & Tech 40.
[79] Li, *supra* note 49 at 33.
[80] Competition & Markets Authority, *supra* note 9 at 3.
[81] Marc Bourreau, Alexandre de Streel & Inge Graef, *Big Data and Competition Policy: Market power, personalised pricing and advertising* (Brussels: Centre on Regulation in Europe, 2017) at 48.
[82] Adapted from the *Telecommunications Act*, SC 1993, c 38, s 72.002(1).
[83] Todd L Archibald & Kenneth E Jull, *Profiting from Risk Management and Compliance* (Canada: Thomson Reuters, 2023) at §7:5.
[84] *Ibid* at §7:9.
[85] *Ibid* at §7:4.
[86] *R v Michaud*, 2015 ONCA 585 at para 102, leave to appeal to SCC refused, 2016 CanLII 24866 (SCC).
[87] Archibald & Jull, *supra* note 83 at §7:5.
[88] *Ibid* at §7:6.
[89] Seele et al, *supra* note 21 at 710.
[90] Douglas Clark, "Health & Personal Care Leads Growth of US Ecommerce" (last visited 25 November 2024), online: <emarketer.com/press-releases/health-personal-care-leads-growth-of-us-ecommerce/>.
[91] Seele et al, *supra* note 21 at 709.
[92] Archibald & Jull, *supra* note 83 at §7:4.
[93] *Competition Act*, *supra* note 36, s 78(1)(k).
[94] *Ibid*, ss 52, 74.01(1)(a).

[95] Chapdelaine, *supra* note 3 at 28.
[96] Statista, "E-commerce in Canada—statistics & facts" (1 July 2024), online: <statista.com/topics/2728/e-commerce-in-canada/>.
[97] Schwartz et al, *supra* note 18 at 45.
[98] *Ibid* at 44.
[99] See *Telecommunications Act*, SC 1993, c 38, s 72.001. See also *Occupational Health and Safety Act*, RSO 1990, c O.1, s 66 [OHSA].
[100] *Guindon v Canada*, 2015 SCC 41 at para 76.
[101] *Ibid*.
[102] *OHSA*, *supra* note 99.