WORLD ECONOMIC FORUM

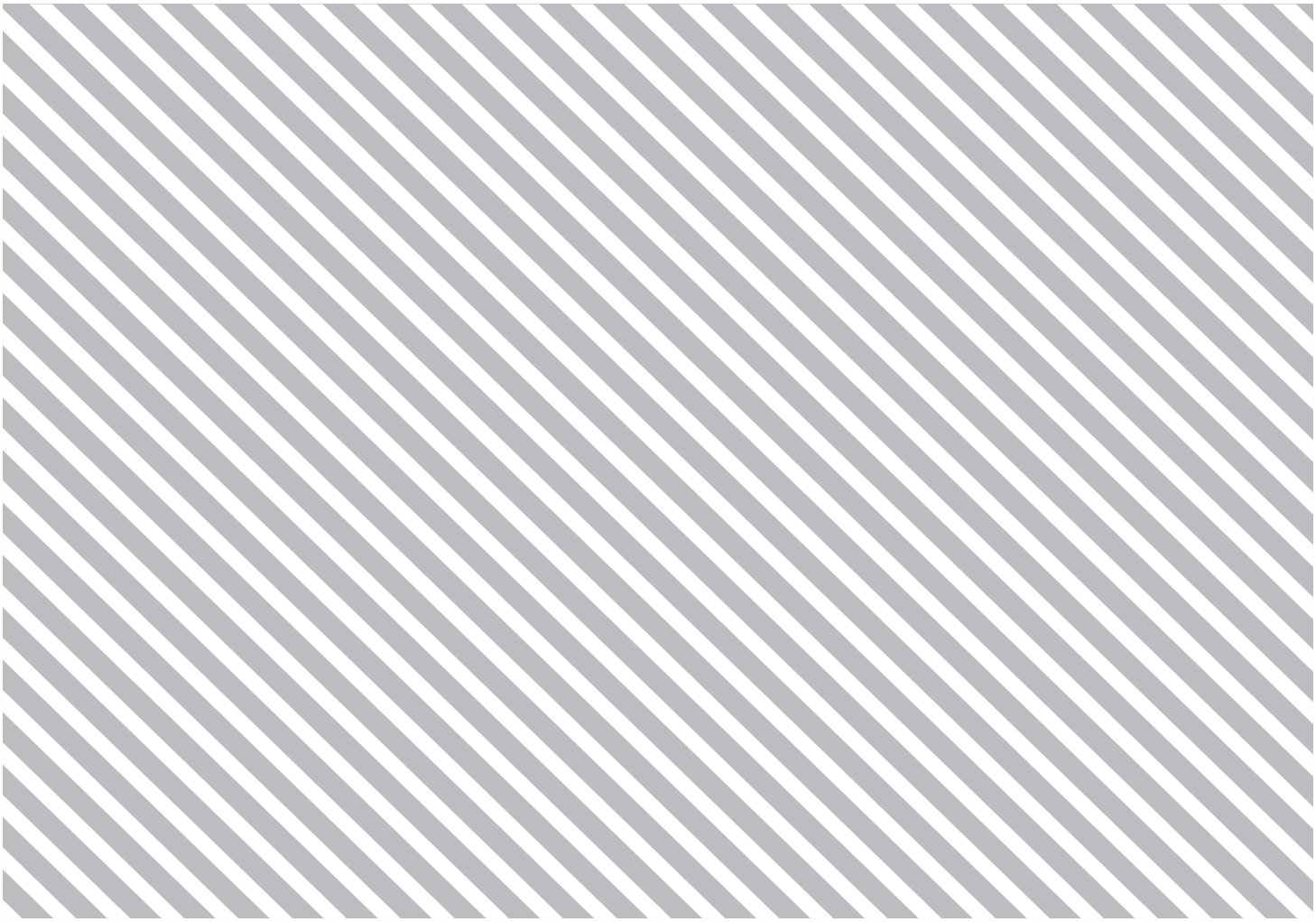
COMMITTED TO IMPROVING THE STATE OF THE WORLD

White Paper

The Global Governance of Online Consumer Protection and E-commerce

Building Trust

March 2019



World Economic Forum
91-93 route de la Capite
CH-1223 Cologny/Geneva
Switzerland
Tel.: +41 (0)22 869 1212
Fax: +41 (0)22 786 2744
Email: contact@weforum.org
www.weforum.org

Authored by:
Ioannis Lianos, Despoina Mantzari, Gracia Marín Durán, Amber Darr and Azza Raslan, Centre for Law Economics and Society, Faculty of Law, University College London (UCL)

Contents

Introduction: Why does this matter?

Since the mid-1990s, e-commerce has become an important feature of commercial activity throughout the world.[1] However, hurdles to e-commerce do still exist,[2] notably in an international context for consumers. Cross-border e-commerce accounted for just 7% of total online business-to-consumer (B2C) sales in 2015, according to the United Nations Conference on Trade and Development (UNCTAD), while business-to-business (B2B) represents the lion's share of a growing $25.3 trillion e-commerce market.[3] One important limiting factor in both developed and developing economies is the perception that cross-border online transactions and delivery are less secure, and remedies do not exist for when something goes wrong.

Generally speaking, trust between consumer and supplier or retailer is a bigger issue online than it is offline.[4] There is usually limited face-to-face contact, yet goods and services are purchased. Traditional shopping provides a social context that facilitates the transaction: It mostly involves a simultaneous exchange of goods and money, interactions with staff and "visual cues", which permit the consumer to test the retailer or suppliers' professionalism. Conversely, online transactions are "stretched over space and time", and "dis-embedded" from a relation of personal trust and physical presence.[5] Though virtual assistants and, soon, virtual reality may help, the experience of transacting online clearly has some differences from more traditional forms.

In this environment, consumers are asked to disclose sensitive information and personal data either to a retailer, online intermediary or digital platform. Credit card details can be hacked or personal identification leaked.[6] When personal data-related stories make headlines, consumers may be dissuaded from entering into e-commerce transactions in the future. Increasing numbers of "mobile-only" consumers and other new technologies such as smart devices may raise fresh security and data treatment issues.

Many governments have issued regulations to address online consumer and data protection, fraud and related issues of competition within their jurisdictions. Some entrust independent regulatory bodies, such as consumer protection, data protection or competition authorities, with the task of overseeing sound online markets. A hoped-for outcome is to boost trust, if not vis-à-vis the specific retailer (personal trust), at least regarding the institutional framework regulating e-commerce (institutions-based trust). Independent regulatory bodies' ability to sanction any opportunistic behaviour can also serve as a mechanism to build higher levels of trust. In some countries, a separate payments regulator is also in place that might touch on consumer issues related to digital payments. In other cases, calls have been made to establish a specific e-commerce regulatory authority.

The difficulty of developing adequate online trust increases when cross-border transactions are made – particularly if one of the parties to the transaction is from a jurisdiction with a high incidence of counterfeits or a weak rule of law. If consumers perceive that they do not benefit from the same level of protection or have access to equivalent remedies in a foreign market – such as returns, the proper handling of sensitive personal data or adequate e-payment security – their confidence in cross-border transactions may decrease.

Lack of familiarity with another country's legal system for consumer and data protection may also affect trust.[7] In some cases, consumers may not know they are shopping online across borders, potentially leading to damaged trust if issues arise. One study by consumer group Which? in 2017, for example, indicated that 21% of consumers buying from an online retailer from outside the EU were unaware of that fact.[8]

In a CIGI-Ipsos online survey of 24,225 internet users in 24 developed and developing countries, 22% of online respondents said they never shop online. Of these, 49% gave lack of trust as the reason.[9] Within the EU, consumers have expressed less confidence about e-shopping across borders (38% felt confident in 2014) than about shopping within their member state (61%), according to the European Commission Consumer Conditions Scoreboard. The scoreboard also found that, in 2014, only 15% of consumers reported buying goods or services via the internet from other EU countries, while 44% bought from national sellers or providers.[10] Higher cross-border online confidence, and thus conversion from browsing to sales, is probably even less likely where countries are not part of a single market with a common body of law.

Different rules on customs procedures, duties, taxes and recognition of e-signatures that add complexity may equally fuel consumer discomfort with international e-commerce. It should be noted, of course, that assessing the impact of regulatory divergence on the level of trust is a complex exercise. Care is needed to distinguish between legal/institutional factors that are likely to affect the level of trust in e-commerce and other sociocultural and/or economic factors at play.[11]

Low levels of cross-border trust have an impact on export opportunities, particularly for small and medium sized enterprises (SMEs) in developing countries, and leads to lost revenue sources for e-commerce platforms, payment providers and logistics firms. Conversely, less regulatory divergence in online consumer protection laws can make it easier for small businesses to engage in e-commerce in the first place. As explained in a recent International Trade Centre (ITC) report:

Though designed to reinforce potential customers' confidence in e-commerce, law and regulations protecting end users can have the opposite effect, insofar as they may make it more complex, time-consuming and costly for companies, especially SMEs, to trade across borders via electronic means. Indeed, the variations in consumer protection laws across different target markets have two unfavourable outcomes. First, they often generate legal uncertainty, especially for e-traders who lack the necessary human and financial resources to carry out proper market intelligence on what local consumer protection laws and regulations dictate in each target market (e.g. as regards the type of information websites should or should not contain). Second, they may create a more costly, time-consuming and cumbersome adaptation process for websites, which can be particularly burdensome on SMEs, especially when businesses are unsure about what is actually required of them.[12]

Governments have sought to collaborate on these cross-border challenges. Various competition, consumer protection or data protection agencies coordinate across jurisdictions, eventually via regional or international economic networks and institutions.[13] According to an OECD survey, 87% of 31 economies surveyed have frameworks to enable cooperation related to consumer protection among national authorities.[14]

Some preferential and regional trade agreements (PTAs/RTAs) have included provisions on online consumer protection. These developments have fed into global trade conversations on "facilitating e-commerce", online retail and digital trade writ large. Discussions to date have largely been associated, though not synonymous, with the development of an interoperable and non-protectionist e-commerce legal infrastructure.

For some policy-makers, the need to include consumer protection in a new global trade deal stems from the view that e-commerce trust is forged not just though the bilateral relationship between a consumer and a supplier or retailer, but is intrinsically related to broader governance frameworks for cross-border e-commerce. A certain level of "system trust" needs to be developed at a global scale for e-commerce to deliver more opportunities. For other governments, new rules could clarify uncertainties on the extent to which domestic consumer protection or data protection laws bind retailers established in other jurisdictions.

Of course, governments are not alone in trying to tackle consumer protection-related issues in cross-border transactions. Private-sector mechanisms have been developed over the past decade by online platforms aiming to enhance the service provided by their specific network or through various collaborations. Other market-based mechanisms may also enhance the level of trust in online transactions – for instance, robust insurance, grievance redress and guarantee mechanisms – protecting the system trust in online transactions. In future, it is also possible that more decentralized technological solutions will develop, guaranteeing consumer protection and privacy through distributed ledger technologies and artificial intelligence (AI). Consumer organizations and networks also aim to limit challenges and improve the global e-commerce experience.

The remainder of this paper offers a brief overview of the online consumer protection landscape and the actors within it. The paper identifies specific forms of online consumer protection and outlines efforts to boost regulatory coherence at the regional and global level – including through trade policy.

Note that included within the scope of "consumer protection" as conceptualized by this paper is the concept of "personal data protection". We readily recognize that while the two concepts overlap, they are not synonymous. They touch upon different policy priorities – the first on how to treat personal information and the second on how to ensure the soundness of online, remote transactions. Even within a single government, data and consumer protection authorities may not be one and the same. That said, the paper chooses to embrace a broad conception of the term because both aspects affect how secure and confident consumers feel transacting online.[15]

Understanding the landscape

As a rule, consumer protection legislation aims to safeguard the economic interests of consumers, empower them with free and informed choice and bestow rights if problems arise. Regulatory instruments, embodied in legislation, can specify a duty of information, a total prohibition of misleading and aggressive practices, a prohibition of unfair contract terms in certain types of contracts and so on. The same is the case in an online context, though legislation often needs to be updated to clarify coverage, as outlined in more detail in the next section.

Most countries around the globe have a legislative framework for consumer protection and many have taken steps to cover online transactions. In part, this has been delivered through "regionalization" of consumer law and policy, with coordination taking place – to a greater and lesser extent – between the EU, ASEAN and APEC, or common approaches by the BRICS nations (Brazil, Russia, India, China, South Africa).

At the international level, some advances have been made through the United Nations Commission on International Trade Law (UNCITRAL), the United Nations Conference on Trade and Development (UNCTAD), the Organisation for Economic Co-operation and Development (OECD), the International Consumer Protection and Enforcement Network (ICPEN).[16] Civil society groups including Consumers International (CI)[17] and consumer groups worldwide complement the picture. In a global economy, digital or otherwise, consumer law has necessarily become an increasingly supranational phenomenon. Regulatory divergences and friction remain, however, suggesting overall governance has not kept pace with market developments.

Box 1: Global status of online consumer protection rules

UNCTAD finds that to date around 52% of countries have relevant online consumer protection legislation. No data is available for a further 32%, while 10% have no legislation in place. The organization runs a Cyberlaw Tracker, which also maps relevant e-commerce legislation worldwide related to data protection, cybercrime laws and e-transaction rules. Across all of these areas, adoption levels are the lowest for laws protecting consumers online. Around 78% of countries have e-transaction laws in places and 58% have privacy laws.[18]

Online consumer protection rules can be private, public or mixed systems of governance. Some jurisdictions consider that industry self-regulation and market supervision by consumer associations best achieves online consumer protection.[19] Here, policy-makers consider that firms often provide information, including on available forms of redress, to customers to enable informed choices. Firms publish their own refund, return and cancellation policies and often organize customer feedback and evaluation mechanisms – with the latter being an important characteristic of the peer-to-peer economy. Consumer associations may flag possible violations of rights and fraudulent or deceptive activity.[20]

Other policy-makers choose to regulate more explicitly. Governments may adopt laws and regulations that provide e-consumers with rights regarding the return and cancellation of goods and services or relating to the protection of data privacy. Governments may also put in place different enforcement systems for these consumer rights: public, semi-private, offline or online – including online dispute settlement procedures (see Annex 1).[21]

Frameworks for the protection of personal information are also considered part of the online consumer protection toolkit by many stakeholders. Although not exclusively aimed at protecting consumers, given that personal data may not only relate to a B2C exchange and not all data protection subjects are consumers, the evidence suggests data protection legislation plays an important role in enhancing online consumer trust. In a 2017 KPMG online shopping survey of more than 18,000 consumers in 50 countries, 41% of respondents said that having control over how their personal data is used was more likely to make them trust a company, especially in North America, Europe and South Africa.[22]

Although early studies found that individuals will perform a "privacy calculus"[23] before disclosing information necessary to complete an e-commerce transaction, more recent discussion has shown there is some cognitive dissonance between consumers' online behaviour (revealed preferences) and their stated preferences for privacy, leading to the "privacy paradox". Users may value privacy, but do nothing to protect it.[24] Recent research also highlights the bounded rationality of consumers when performing this privacy calculus – in other words, consumers lack the expertise to compare the costs and benefits of sharing personal information.[25]

Further, despite privacy notices, individuals may not always be aware of the data harvesting to which their personal information is subject, as they rarely, if ever, read websites' terms and conditions (T&Cs) of service due to the length, legalistic language and a "take it or leave" it approach.[26] For want of any better alternative, "tick, click and hope for the best" sums up most consumers' attitude. Through the internet of things (IoT), users may in future allow smart devices to engage in online transactions on their behalf based on learned preferences. A more systematic use of digital assistants might require default or adapted consent mechanisms.[27] Conversely, tech advances could also lead to better results for consumers if, for example, AI formed by learned consumer patterns was used to form buyer coalitions that seek better terms.[28]

The rapid emergence of "data-centric" global business models – where the perceived underlying exchange deals in products or services for personal data – has accelerated

debates worldwide on how policy-makers should approach the data privacy topic in the context of digital commercial transactions. The EU has put in place a General Data Protection Regulation in Europe (GDPR) that ensures the extraterritorial protection of data subjects in the EU from conduct taking place outside the EU.[29] There are also moves in Brazil, India and the US, among others, to introduce stronger data protection rules.[30] Some jurisdictions have developed mechanisms for guaranteeing the international transfer of personal data where adequate conditions are met – this is the angle of interest to the trade community. Discussion in this area is likely to evolve.

Regulatory instruments in play

In theory, online consumer protection legislation has the potential to regulate almost all aspects of a consumer–business relationship, namely the "pre-purchase" stage (including advertising, information requirements, unfair commercial practices etc.), the "purchase" stage (including unfair contract terms, online payment security etc.) and the "post-purchase" stage (including dispute resolution, redress requirements etc.).[31] Legislation can also impose pre-contractual, contractual and post-contractual obligations on suppliers to remedy the unequal bargaining position and informational asymmetry of the consumer vis-à-vis the supplier.

In the pre-sale phase, this may be done through rules regulating online payment as well as those governing the delivery of a product or service. More specific online consumer law provisions, particularly various anti-spam laws protecting consumers from unsolicited commercial and marketing email communications, may also apply. Additional rules may cover activities that take place after buyers have made an online payment and sellers have delivered a product or service.

In some cases, e-commerce activities are different from offline commercial transactions. For example, third parties in an online marketplace, rather than the online platform itself, may engage in misleading practices. E-commerce transactions can be "bilateral", signifying that they are conducted between businesses or businesses and the consumer, or "triangular", taking place via online platforms. When consumers conclude a contract via an online platform such as eBay, Mercado Libre or Airbnb, the platform is usually not party to the contract between the consumer and the supplier of the goods and services; instead, it acts as an intermediary.

Although some countries have already established regulatory regimes tailored to platform commerce, these differ widely with respect to the obligations imposed. For instance, China places extensive responsibilities on e-commerce platforms to the extent that platforms will be held liable if they fail to provide information on offending vendors,[32] whereas the US and EU place more responsibility on users.

Box 2: Digital platforms and contracts

Passenger transportation services such as Uber and Lyft have T&Cs aimed at standardizing requirements for performance quality and attracting clients with brand or service consistency. In comparison to Uber, Airbnb allows its users more freedom to determine important characteristics of the contract. In turn, different approaches can influence what legal responsibilities might be attributed to the platform provider. In cases where the platform appears as a party to the contractual relationship, the question arises as to whether it should be held liable in the event of non-performance of the obligation on the part of the supplier.

Source: Authors' own

Table 1 briefly outlines the typical instruments used to date to address challenges in three online consumer protection stages. Additional detail is provided in Annex 1. As noted, some consumer protection remedies involve the private sector in the regulatory process, which can be relevant across the board.

Industry self-regulation (ISR) agreements are gaining in importance in e-commerce as the rapid pace of innovation with the development of new products and services may raise consumer protection issues that cannot be adequately addressed by existing regulations.[33] The International Organization for Standardization (ISO) first published guidelines for B2C e-commerce in 2013. Co-regulation may be another option, to the extent that a government involves itself, for example, in providing a framework to enforce standards or codes of behaviour developed by industry.[34] The industry may also work with other stakeholders, such as groups representing consumers.

Table 1: Online consumer protection instruments

Stage	Challenge	Remedies
Pre-purchase	Information asymmetry: Consumers may not know the identity and location of an online product provider	Public and private tools, including descriptive information regarding sellers, price comparison websites, mandatory disclosure statements
	Unfair commercial practices: E-commerce can involve aggressive marketing techniques, including incomplete provisions of information, or misleading advertising	Public tools include rules for fair, clear and transparent information; investigations on deceptive pricing schemes
	Unsolicited electronic commercial communications (spam): May be sent to potential consumers via email, messenger services, social networks and text messages, raising issues about privacy and trust	Rules ensuring that consumers are protected against unsolicited communications, can involve an "opt-in" consent requirement to send messages
Purchase	Electronic contracts: Jurisdictions need legislation that recognizes the validity of a contract concluded online	The United Nations has developed model laws for e-transactions and e-signatures
	Contract terms: Define the rights and duties, but the concept of "fairness" in T&Cs differs across jurisdictions as well as access to justice. T&Cs may often be too long for consumers to read – for example, Consumers International estimates it would take the average person 76 working days to read all of the T&Cs encountered online in one year. Intermediary sites may also have T&Cs for sellers	Requirements to draft contract terms in plain and intelligible language
	Confusion on seller location and status: Intermediary online platforms adopt varying approaches towards displaying information about location of sellers. Some consumers may also believe they are buying from an online marketplace when they are entering into a contract with a third-party supplier, who may not meet their expectations of professionalism. Identifying the seller also matters when a product turns out to be faulty	Requirements for online marketplaces to inform customers on who the contract is being concluded with; duties to inform the consumer on the contractual role of the platform; exemptions for intermediaries from secondary liability if they are not knowingly hosting illegal content or activities
	Cooling-off period: E-commerce changes the pace of exchange. Consumers may want a period in which to cancel mistaken online orders. The exact length of this period varies between jurisdictions. Product prices may also move while a consumer is online	Some countries offer time to cancel or return an order made online, though this varies greatly
	Online payment security: A survey by PWC found that e-shoppers around the world are worried about the security of online payments	Requirements for tiered levels of security and authentication based on payment risk or company size. Some international recommendations call for collaboration on minimum levels of consumer protection in this area, such as on limitation of liability for unauthorized use, chargeback mechanisms etc.
	Personal information protection: misuse of personal information or data harvesting practices can affect consumer confidence in using online tools for e-commerce or otherwise	Consumer protection laws may require companies to provide customers with transparent, clear and easily accessible information on what personal information they consent to share and for what purpose. Laws can also allow for consumer opt-outs from data harvesting for advertising and/or marketing purposes. In some jurisdictions, data protection rules mostly refer to data security, and do not encompass privacy concerns

Post-purchase	Liability rules: Cover the rights of consumers to expect goods are delivered safely and in a timely manner. In a triangular e-commerce transaction, however, the consumer may not be clear when the platform operator is liable and when it is the seller on the line. Liability issues at stake include responsibility for faulty or counterfeit goods, late or non-delivery. Online platform T&Cs usually underline that they are not party to supplier-customer contracts, acting instead as facilitators or matchmakers. Platforms often provide standard T&Cs for suppliers' contract of sale or service (see example in Box 3). Approaches to liability vary across jurisdictions, and debates on the responsibility of online marketplaces are in some cases ongoing	Public and private tools include: Standard T&Cs for contract of sale; clarifications on who is responsible for product or service delivery and complications
	Dispute resolution: A critical aspect of e-commerce. However, dispute-resolution options available to consumers vary across jurisdictions, and there is still no consensus as to whether dispute resolution for online transactions should be regulated by governments or self-regulated by the private sector. Many online platforms have their own systems for dispute resolution	Some efforts to streamline judicial proceedings to make these more suitable for consumer e-commerce disputes; calls from business, government and consumer representatives to develop fair, effective and transparent self-regulatory policies and procedures, include alternative or online dispute-resolution mechanisms (ADR/ODR), able to address cross-border issues. A few jurisdictions have implemented these mechanisms, though they are sometimes focused only on domain-name dispute resolution, and do not necessarily include an extraterritoriality component. Even when suitable ADR/ODR mechanisms do exist, usage and effectiveness can be undermined by capacity constraints, particularly in developing countries. Some successful examples have been deployed, however, notably in Latin America

Source: Authors' own

Cross-border solutions: What's been done to date

Governments are increasingly discussing the facilitation of cross-border e-commerce as a new dimension of trade, which, for the reasons outlined in this paper, should include a focus on raising systemic consumer trust as well as reducing commercial friction. For online consumer protection issues specifically, regulatory cooperation initiatives undertaken in the UN or OECD may provide useful "soft law" touch points for trade policy. ICPEN offers a similar function through the socialization of consumer protection agencies. The following section explores the strengths and challenges of each approach.

International 'soft law'

International convergence efforts for online consumer protection have taken place in non-trade arenas – typically building on initiatives aimed at offline protection. For example, in 1985, the UN General Assembly adopted the Guidelines for Consumer Protection (UNGCP), which were subsequently revised in 1999 and 2015.[35] The progress made is important for those focused on facilitating new types of digital trade – particularly in a way that builds system legitimacy and trust.

The guidelines, which apply to B2C transactions, indicate general principles for effective consumer protection legislation and good business practice, and provide guidance on implementation and encouragement towards international cooperation. Topics covered include transparency and disclosure, consumer privacy and data security, secure payment mechanisms and dispute resolution and redress. The aim is not to reduce regulatory divergence as such, but to ensure a minimum level of consumer protection in each jurisdiction. Member states are encouraged to avoid measures stemming from the guidelines from becoming barriers to international trade.

The guidelines do consider the interests and needs of consumers in developing countries in terms of imbalances in economic terms, educational levels and bargaining power. The guidelines emphasize the need to protect vulnerable and disadvantaged consumers. UN member states should develop, strengthen or maintain strong consumer protection policies that consider the guidelines and other relevant international agreements – though states are also free to set their own priorities.

The most recent update to the guidelines included e-commerce, particularly around the parity of treatment between online and offline consumers, and consumer privacy protection. A group of experts now meets regularly to support the guidelines' implementation. In the past year, the group has exchanged techniques by consumer protection agencies in relation to e-commerce, covering misleading advertising, consumer education, business guidance and cross-border cooperation.

OECD members are also active in this area, adopting one of the first international instruments for consumer protection in electronic commerce in 1999, known as the "1999 Recommendation". Following increased interest in the digital economy, the OECD revised this instrument to address new trends in 2016 in the broader areas of non-monetary transactions, digital content products and mobile devices.[36] It sets out guidance on advertising and marketing practices to reduce the possibility of businesses exploiting the special characteristics of e-commerce. In addition, it outlines detailed rules concerning online disclosures, the confirmation processes for orders and the protection of e-consumers' privacy and security. A specific chapter covers payment issues, reminiscent of the EU Payment Services Directive, calling for, for example, a limitation of liability for unauthorized use and chargeback mechanisms. The update covers consumer-to-consumer (C2C) transactions as well as other forms.

The recommendation also encourages the development of effective co-regulatory and self-regulatory mechanisms that help to enhance trust in e-commerce, including the promotion of effective dispute-resolution mechanisms. Most recently, the OECD has focused on behavioural advertising[37] as well as consumer protection issues arising in the context of the sharing economy.[38]

Global cooperation is particularly relevant for cross-border e-commerce. In the 2016 Recommendation, governments are invited to facilitate communication, cooperation and, where appropriate, joint initiatives to improve consumer protection. Concrete steps outlined include information sharing, investigative assistance (while avoiding duplicating efforts), making use of international networks and entering into bilateral or multilateral agreements as appropriate. The initiative builds on earlier efforts by the OECD to promote cooperation in regard to online consumer protection issues.[39]

The G20 has pursued similar efforts – such as endorsing the High-Level Principles on Financial Consumer Protection in 2011 and the G20/OECD Policy Guidance on Financial Consumer Protection Approaches in the Digital Age in 2018. The German G20 presidency in 2016, meanwhile, held an inaugural consumer summit that endorsed ten policy recommendations, including: equal rights online and offline; digital providers being held to account; affordable and good-quality internet access for all; access to easy-to-understand information on digital products and services; clear and fair terms of use; an increase in digital education and awareness; protection against fraud and abuse; control over personal data and privacy; effective redress and damages claims; and promotion of competitive markets.[40]

ICPEN, formerly the International Marketing Supervision Network (IMSN), facilitates the exchange of information between relevant authorities, publishes guidelines and has a complaint site to record online scams. The network provides

an opportunity to build a soft consensus on common approaches – a method used in other policy fields, too, such as the International Competition Network's approach to competition law and authorities.

Soft law may be a step in the right direction. It has the potential to achieve functional-equivalent regulatory convergence on consumer protection principles. A non-binding approach may also allow for the description of detailed principles, subsequently implemented by consumer protection agencies, knit together as a community of advocates for consumer protection. A downside is that soft law may have limited effects in addressing consumer distrust in poor regulatory environments already in existence – particularly those where domestic reform is unlikely.

The WTO option

Many trade experts argue that WTO rules make no distinction between the different means (whether physical or online) through which goods and services are traded.[41] Various WTO dispute settlement reports have confirmed that the market-access commitments and non-discrimination obligations found in the General Agreement on Trade in Services (GATS) extend to the electronic supply of services.[42]

Nonetheless, WTO members initiated a work programme as far back as September 1998 to better understand the implications of WTO rules on emerging online modes of cross-border trade.[43] Discussions in the work programme over the past two decades, however, have been of limited relevance to online consumer protection. For the most part, the focus has been on trade-liberalizing measures (e.g. market-access commitments, non-discrimination etc.) and related classification issues, rather than on regulatory tools to build consumer trust in e-commerce. To some extent, this is not surprising given the nature of the WTO – an organization that promotes international trade liberalization rather than setting standards or regulatory harmonization on trade-related matters.

The increasing prominence of digital trade led to developments in two parallel discussion tracks at the organization's 11th Ministerial Conference (MC11) in December 2017. At the multilateral level, the work programme was rolled over with a focus on existing WTO rules, while 70 WTO members adopted a Joint Statement on Electronic Commerce, agreeing to undertake exploratory work towards future negotiations.[44] Within this "plurilateral" process, several WTO members put forward proposals that touched on online consumer protection, as summarized in Table 1. In January 2019, 76 WTO members, responsible for over 90% of global trade, confirmed their intention to begin negotiations on the trade-related aspects of e-commerce.

Table 2: WTO proposals on online consumer protection (2018)

WTO member (s)	Online consumer protection	Agency cooperation	Personal information protection
The Separate Customs Territory of Taiwan, Penghu, Kinmen and Matsu			WTO members to commit to not adopting or applying measures that hamper the cross-border transmission of information, unless under exceptional circumstances; WTO members to agree to a set of principles or guidelines that indicate when exceptions to information transmission may be legitimate and how to apply such regulatory measures on a transparent and non-discriminatory basis
Russian Federation	Protect online consumers' rights at a level no less than provided in offline commerce; recognize important online consumer rights in e-commerce; ensure security of cross-border e-commerce; encourage the private sector to engage in good business practice; define measures that can counter cross-border violations of consumer rights and safety; create a digital platform to share information on unsafe online goods and services	Set basic principles for cooperation and information exchange on cross-border trade for competent authorities and develop unified approaches for cooperation and mutual aid to prevent dishonest activity in e-commerce	Standards for personal data transmission in the supply of payment services; conditions for personal data treatment, including storage, confidentiality and security
European Union	Adopt or maintain measures that contribute to consumer trust; adopt or maintain measures that protect consumers against unsolicited commercial electronic messages (i.e. "spam") and agree to a set of broad technology-neutral obligations including consent, prevention, identification and recourse	Recognize the importance of cooperation between national consumer protection agencies and other relevant bodies	
New Zealand	WTO members commit to minimum legal frameworks to prevent the use of misleading or deceptive practices online; put in places measures to address spam		WTO members commit to establishing or maintaining a legal framework to protect personal information of electronic commerce users
Argentina, Colombia & Costa Rica	Negotiate to address regulatory issues		Affirm WTO members' right to regulate to ensure the protection of individual privacy, security and confidentiality of information

Brazil	WTO members to protect end users against unsolicited direct marketing communications; ensure direct marketing, where allowed, is clearly identifiable as such; common understanding on return periods; a list of objectives WTO members should pursue or maintain to enhance consumer trust, such as measures that prohibit charging consumers for services not requested or for a period in time not authorized	WTO members recognize the importance of cooperation between respective national consumer protection agencies or other relevant bodies	WTO members to adopt or maintain a legal framework that provides for the protection of persona data of individuals, taking into account the principles and guidelines of relevant international bodies; encourage the development of mechanisms to promote compatibility between different privacy regimes; outline a set of criteria where the international transfer of data is allowable; WTO members to ensure online platforms are responsible for personal data stored and managed
Singapore	Adopt measures/laws to protect online consumers from fraudulent and deceptive commercial activities; adopt and maintain measures to address spam	Promote international cooperation between consumer protection agencies	Adapt or maintain measures that offer protection for personal information

Source: Authors' analysis of proposals made in the e-commerce joint statement discussions in 2018.

Although the WTO proposals to date converge on the importance of consumer-related issues, they are vague about the substantive content of the "set of principles" or "minimum legal frameworks" that ought to be encouraged or required by WTO law. However, the early stages of discussions may offer a partial explanation.

Non-governmental organizations, such as Consumers International, have also outlined a "checklist" of elements critical for any international e-commerce deal. Under the banner of "informed choice", consumers should have a clear and accurate presentation of information, transparency on subscription service payments and clarity on the location of retailers. For increased "access and inclusion", the needs of vulnerable and disabled consumers should be considered, with responsible marketing warnings and age verification checks also emphasized. "Effective protection" should be given in the manner of other forms of commerce, with consumers able to explicitly agree to a purchase and receive a receipt. Consumers should have access to fair and effective dispute resolutions if something goes wrong. "Product safety" should be pursued with clear warnings and information on safe use; "data protection" should be of a high standard in both substantive and procedural national laws. "International cooperation" should be encouraged, including through the UN, ICPEN, OECD and regional bodies, and any e-commerce negotiating process should be transparent and should involve multistakeholder dialogue.[45]

Questions remain as to whether the WTO is the most appropriate forum for adopting such international e-commerce agreements and for regulating online consumer protections. On the one hand, the WTO may seem better placed to tackle this issue than other international or regional governance structures: It is the backbone for international trade governance; it benefits from a quasi-universal membership; it benefits from the flexibility of a "plurilateral approach" to rule-making when needed; and, in theory at least, it has a relatively sophisticated and effective dispute settlement system – notwithstanding the ongoing Appellate Body crisis.[46] In policy terms, divergence in domestic consumer laws could be a non-tariff barrier to cross-border online transactions, and hence qualify as a trade-related concern for the WTO.

On the other hand, the WTO presently has limited experience in promoting regulatory convergence on trade-related matters. Only the Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS Agreement) has unquestionably moved in the direction of positive integration, by prescribing the minimum standards of intellectual property protection in both substantive and procedural terms – building on preexisting World Intellectual Property Organization (WIPO) conventions. WTO rules on technical barriers to trade and on sanitary and phytosanitary measures encourage harmonization of relevant international standards developed by other competent international organizations[47] or the mutual recognition of domestic regulations.[48] These provisions are qualified, however, and make it the choice of each WTO member to regulate (or not) at the level of protection it deems appropriate.

Some progress towards standard-setting was arguably made, however, through the "WTO Telecommunications Reference Paper on Regulatory Principles". Adopted in 1996, the document set out common principles for a regulatory framework that were considered important as the telecommunications sector transitioned from dominance by state-owned monopolies to one where competition is prevalent.[49] The aim was to minimize divergence by stipulating the vital elements for an effective regulatory framework on telecommunications services. Some 82 members have integrated the reference paper into their respective GATS Schedules of Commitments to make its principles legally binding.

WTO members engaging in plurilateral e-commerce negotiations could consider this approach, allowing them to identify the most effective regulatory practices for online consumer protection. A common set of detailed minimum international standards for implementation by the participating countries could be outlined. Doing so could help boost consumer confidence in e-commerce in parallel with easing the costs that hold back small businesses selling online in the first place – encouraging a virtuous circle between demand and supply.

The approach does have some disadvantages. First, as with the Telecommunications Reference Paper, only a limited number of WTO members might commit to be bound by the minimum standards in online consumer protection. Governments that are already digital-savvy may be the only ones to participate in the process, making the regulatory improvements brought by WTO bindings relatively limited. Second, a reference paper approach could set a high bar, particularly for developing countries that may not yet have the resources to adopt and implement online consumer protection laws. WTO negotiations could remedy this by offering technical assistance to support lawmaking and implementation. Third, drafting of minimum online consumer protection standards cannot provide a definitive solution to the problem of regulatory friction and the subsequent consumer mistrust in e-commerce, since it will not lead to harmonization. It would still be possible for some WTO members to impose higher online consumer protection standards, therefore allowing some degree of regulatory diversity to remain.

Additional questions exist in regard to enforcement. The WTO dispute-settlement system is state-to-state.[50] If a WTO member violated its regulatory commitment to online consumer protection, affected individuals in another country would need to rely on his or her home state to bring a challenge.

The regional deal option

An increasing number of regional or preferential trade agreements (PTAs) cover cross-border e-commerce.[51] According to research conducted by the WTO Secretariat, of the 275 PTAs that were in force and notified to the WTO as of May 2017, 75 contain provisions specific to e-commerce. Of these, 65% include online consumer protection provisions,[52] about 58% contain provisions on personal information protection and 28% cover unsolicited commercial electronic messages.[53]

In most cases, the PTA's dispute-settlement mechanism would apply to the e-commerce chapter, with only ten agreements excluding some or all relevant provisions.[54] However, as in the case of the WTO, these are traditional state-to-state dispute-settlement mechanisms, with only three PTAs providing for alternative mechanisms to resolve cross-border e-commerce disputes.[55]

The legal strength and enforceability of these provisions varies significantly. On the stronger side of the spectrum are provisions that are clearly mandatory and enforceable. An example is the PTA provisions dealing with the adoption of personal information protection measures,[56] with about half requiring each party to adopt or maintain personal information protection laws and often including a reference to international standards and the criteria of the relevant international bodies (albeit with qualified language: "should take into account").[57]

At the weaker end of the spectrum are provisions framed in language seeking the most effective methodologies that may be difficult to enforce in practice. Online consumer protection measures,[58] in most cases, fall short of imposing a mandatory obligation.[59] The same applies to PTAs calling for e-consumer protection that is at least equivalent to that provided to consumers in other forms of commerce.[60] Similarly, relatively weak legal terms are used for the prevention of unsolicited commercial electronic messages,[61] with few agreements incorporating a binding commitment.[62]

In some respects, PTAs present prime laboratories for developing new rules among groups of "like-minded" countries on trade-related issues, particularly on topics that have stalled at the WTO.[63] However, consumer-related provisions in PTAs arguably have had limited legal significance to date, despite being an important step forward from a policy or political perspective. To date, many PTAs simply include a provision recognizing the importance of adopting and maintaining transparent and effective consumer protection measures for e-commerce. Very few PTAs mandate the adoption or maintenance of measures to protect consumers in growing digital trade – other than to some extent for personal data protection. Further, even in areas where substantive progress has been or could be made, the PTA option is inherently fragmented and there is no guarantee of regulatory convergence across agreements.[64]

One option for consideration in this respect are the e-commerce consumer protection principles included in recent mega-trade agreements negotiated between regional economic blocs. For example, the Comprehensive and Progressive Partnership for Trans-Pacific Partnership (CPTPP) e-commerce chapter mandates that parties adopt or maintain consumer protection laws that address fraud or harmful online commercial activities (Article 14.7). Parties must also adopt measures for spam that empower recipients to stop reception, require consent or otherwise minimize this form of communication (Article 14.4). International cooperation between national consumer protection agencies in cross-border electronic commerce is also promoted. The CPTPP consolidates and builds off the commitments found in various bilateral PTAs between its members.

Similarly, the United States-Mexico-Canada Agreement (USMCA) requires laws protecting consumers from fraudulent and deceptive online activity (Article 19.7) and strong measures on spam (Article 19.13). The EU-Japan economic partnership agreement also includes a binding commitment on spam focused on prevention, consent, identification and recourse (Article 8.79). In addition, Japan and the EU agree to maintain regulatory dialogue on e-commerce, with a view to sharing methodologies, including in regard to consumer protection, cybersecurity and combatting unsolicited commercial electronic messages (Article 8.80).

Both the USMCA and CPTPP include the requirement for domestic personal information protection regimes and commitments to cross-border information transfers as well as the prohibition of data localization as a condition for doing business. The personal information protection provisions in both instances encourage "non-discriminatory" practices to protect users of digital trade – meaning that a foreign national should receive the same treatment as a national citizen. For some experts, the provision signals a way towards ensuring the extraterritorial application of countries' privacy regimes if built upon in certain ways.[65] By contrast, the Canada-EU Comprehensive Economic and Trade Agreement (CETA) includes a slightly softer requirement that parties "should" adopt measures protecting personal information of e-commerce users (Article 16.4), while the EU-Japan deal "recognizes the importance of adopting or maintaining" measures in this area (Article 8.78).

Of the four, USMCA goes furthest in specifying that personal information protection provisions could use APEC and OECD principles developed in this area, while the others encourage the use of international guidelines more generally. The CPTPP encourages the "development of mechanisms to promote compatibility" between different privacy regimes – citing recognition or international frameworks as options (Article 14.8). Taken together, the four deals cover millions of online consumers. To a degree, each recognizes the importance of personal information protection, and two of these nod to the need for interoperability between regimes.

Provisions on online consumer protection are also included in other regional economic integration models, as suggested above. For instance, the Association of Southeast Asian Nations (ASEAN) was the first developing region to prepare a unified e-commerce legal framework,[66] and has since set out a common strategy for consumer policy as well as an e-commerce trade pact.[67] The ASEAN Committee on Consumer Protection (ACCP) published a *Handbook on ASEAN Consumer Protection Laws and Regulations* in August 2018, aimed at promoting transparency in the consumer protection framework. It provides quick and simple references about the consumer protection frameworks or systems operating in the region, including the establishment of an ASEAN regional online dispute-resolution network.[68]

However, the mega-regional option is no less fragmented than the PTA option, to the extent that it does not guarantee regulatory convergence at a global level (i.e. provisions in mega-regionals on e-commerce still differ, as reflected above).

Next steps

In many respects, e-commerce is a more "de-personalized exchange" than face-to-face contact with its visual cues. Yet it offers huge opportunities for small businesses to reach new customers in ways never previously imagined. Governance frameworks can help raise consumer confidence in a fair marketplace; but in a world of cross-border e-commerce, both consumers and businesses must still contend with the uncertainty and potential costs of divergent approaches.

Global digital platforms offer one avenue for boosting consumer confidence insofar as they assume certain duties and risks in brokering the transaction. However, this places a large responsibility on private actors, and raises questions about transparency and possible concerns about competition if the platform becomes dominant, among other things. Certainly, global and regional platforms can offer important tools, such as alternative dispute-resolution mechanisms, as well as encouraging high standards in business (and customer) behaviour. Public-private initiatives working with governments can also be useful – though are undoubtedly harder to implement on a cross-border basis.

A public governance approach involves two steps: First, ensure countries adopt or upgrade online consumer (and data) protection laws in a way that will keep pace with developments in technology and afford as much protection as that offered to offline consumers. Technical assistance may be helpful in countries where these rules are not yet in place. Further reflection on interoperability, cooperation or extraterritorial coverage may be needed to ensure countries' domestic policy objectives are achieved abroad on the same scale as they are at home – here, creative thinking from the trade policy community may be useful. Second, work towards cross-border cooperation and convergence. Doing so would contribute to system-wide trust and make life easier for small businesses in the global digital economy.

International efforts could be further pursued through UNCITRAL, UNCTAD, the WTO or regional trade deals. These could be on a sliding scale from regulatory convergence to commitments on cooperation among agencies. Any new initiatives will need to be future-proofed against rapid change. The impact of distributed ledger technologies (DLT) on commercial transactions, for example, has increasingly become a topic of discussion. DLT systems can execute "smart contracts" whereby an action is automatically taken – such as payment – once a set of digital criteria is met. OpenBazaar is one example of a blockchain-based peer-to-peer marketplace that also uses cryptocurrencies for settlement.

Playing this scenario forward, unfair business practices may no longer be a main focus of online consumer protection, since identifying conduct might be challenging in a decentralized and pseudonymous network. Regulatory regimes may move to become more "principles-based", relying on dynamic performance standards and a deeper interaction between regulators and online traders within the technological design and business development phase to protect consumers (and merchants). Scaling this approach to a global level will be challenging. But it will also be important given the potential borderless nature of the digital economy.

Annex 1: Online consumer protection regulatory examples

Pre-purchase

Unfair commercial practices

The UK's Competition and Markets Authority (CMA) recently launched an investigation into online hotel booking.[69] In 2016, France updated its rules for fair, clear and transparent information in this area.

In the US, the Federal Trade Commission (FTC) is charged with protecting consumers in the marketplace, outlining prohibitions on companies using unfair or deceptive acts. The agency has investigated new types of deceptive pricing schemes in an online context – such as where the pre-sale price is artificially inflated. Amazon was the subject of such an investigation following its purchase of Whole Foods. The Competition Bureau of Canada, meanwhile, levied a US$1 million fine against Amazon Canada in 2017 for misleading price comparisons.

Unsolicited electronic commercial communications or 'spam'

In Canada, a recent anti-spam law addressed unsolicited commercial electronic messages as well as the installation of computer programs and unfair or deceptive online practices. It is based on opt-in consent to send such messages and is broad in scope compared to approaches taken in other countries. The law also has considerable extraterritorial reach, applying to messages where "a computer system located in Canada is used to send or access"[70] the electronic message.

Purchase

Contract terms

The EU's Unfair Terms in Consumer Contracts Directive refers to the notion of "good faith" to prevent significant imbalances in the rights and obligations of consumers and traders. The directive requires contract terms to be drafted in plain and intelligible language and states that ambiguities should be interpreted in favour of consumers.

Generally, unfair-terms legislation may control the types of T&Cs that businesses can impose; however, the test(s) for unfairness varies from jurisdiction to jurisdiction. For example, the US accepts arbitration and jurisdiction clauses that restrict access to justice (e.g. by barring access to courts or specifying which court can deal with disputes). In the EU, a judge can rule to remove these unfair terms from the contract.

Confusion on seller location and status

The EU's Unfair Commercial Practices Directive applies only if the online intermediary qualifies as a "trader" and "has engaged in a B2C commercial practice directly connected to the promotion, sale or supply of a product to consumers".[71] It is possible to find a breach only if these requirements are fulfilled.

Linked to this, the e-Commerce Directive exempts intermediaries from secondary liability if they do not know they are hosting illegal content or activities and does not subject intermediaries to general obligations to monitor and seek information.[72] The EU also requires online marketplaces to inform customers about the party with whom the contract is being concluded.[73]

Other models concerning a duty to inform the consumer of the contractual role of the platform exist. The Republic of Korea's Act on Consumer Protection in Electronic Commerce is one example, where an online intermediary must explicitly inform consumers that they are not a party to the main supply contract.[74] Another is provided by Brazil's e-commerce rules, which require e-commerce portals to provide clear information about the product or service and supplier from which they are buying.

Electronic contracts

Switzerland and the US do not offer the right to withdraw from a contract, although there are some narrow exceptions in US Federal Law, and many US businesses exceed the legal requirements to offer a right to return goods. In Japan, consumers have a period of up to eight days from the receipt of goods to return them, but this right may be withdrawn by the trader if they specify as such in their T&Cs. In the EU, consumers have up to 14 days; in Malaysia the limit is ten days; in China it is seven days; and in Singapore it is five days. In Brazil, consumers have a "right to regret" and there is a requirement to communicate this to consumers.

Online payment security

Payment authentication standards espoused by the EU call for "strong customer authentication" that demands the relevant banking institution verify the customer's identity through various methods. In the US, the authentication standard is a private-sector initiative known as Payment Card Industry Data Security Standard, which determines authentication requirements based on company size. It has become an integral part of card network contracts with merchants. Alibaba has shaped the way e-commerce payments are made and secured in China through its escrow payment system, Alipay.

Personal information and privacy

In the EU, traders are required, under Directive 98/6/EC (the Price Indication Directive),[75] to indicate the selling price in a way that is easily identifiable and clearly legible. These rules may be implemented so that all parties develop a more

equal level of understanding of the value of the personal information being gathered and processed. For example, where a consumer is provided with a "free service" in exchange for personal data.

The EU General Data Protection Regulation (GDPR) allows any data subject – for instance, an e-consumer – to request the erasure of certain types of information collected by a data comptroller (Article 17). The idea of "privacy by design", as enshrined in Article 25, may also require the consideration of the privacy implications when designing the overall website and e-commerce technical architecture. Remarkably, Article 3(2) stipulates that the regulation may apply extraterritorially to non-EU based organizations if these organizations are monitoring the behaviour of individuals inside the EU.

By contrast, the US has not yet adopted all-encompassing privacy regulations, although this is changing at state level. Instead, the US implements sector-specific data protection laws for consumers, such as healthcare and financial services. In China, data protection mostly refers to data security; it does not encompass privacy concerns.

Post-purchase

Liability rules

In the EU, the trader is responsible for any damage to goods from the time of dispatch until receipt by the consumer. This is not necessarily the case elsewhere and inter-jurisdictional differences can result in grey areas. For example, an Italian consumer may order a product online from a retailer based in China, the product may be dispatched from the warehouse in China to the airport and be transported via courier, the product may be flown to the UK and then delivered to the consumer by the Italian postal service. In some cases, the retailer may be expected to maintain liability throughout the process, seeking compensation from third parties if something goes wrong. In other cases, the third party may be held liable. Within Chinese law, there is no legal obligation to deliver within a particular time frame, nor is there any obligation on the trader to inform consumers about delays or to replace damaged products with an equivalent product. Similarly, there are no such rules in Switzerland, Japan and the US.

Online dispute resolution

The EU has tried to streamline judicial proceedings to make these more suitable for tackling consumer e-commerce disputes. It has also updated legislation and has put "alternative dispute resolution" (ADR) instruments into place. The Directive on Consumer ADR applies to procedures concerning the out-of-court resolution of domestic as well as cross-border disputes used mostly for offline commerce. Regulation 524/2013, the Regulation on Consumer Online Dispute Resolution (ODR), which entered into force on 15 February 2016, introduces specific ODR processes for disputes between consumers and/or traders based in the EU. It focuses on products and/or services that have been bought online, whether they are domestic or EU-based transactions.

In Asia, China has implemented ODR for domain name disputes through the Asian Domain Name Dispute Resolution Center (ADNDRC) and the Online Dispute Resolution Center at the China International Economic and Trade Arbitration Commission (CIETAC). Also, China Commercial Arbitration, run by Guangdong Arbitration Commission, offers online arbitration for e-commerce disputes, while Taobao, a shopping website run by Alibaba, has created its own private consumer ODR system.

In 2002, Singapore launched DisputeManager.com, the first comprehensive ODR service in Asia. Developed by the Singapore Academy of Law and its subsidiary, the Singapore Mediation Centre (SMC), DisputeManager.com offers three main services: e-settlement (an automated ADR process in which the parties make offers and agree to settle once certain conditions are met); online mediation; and neutral evaluation. DisputeManager.com also supports the Singapore Domain Name Dispute Resolution Service, a service similar to ADNDRC but focused solely on resolving Singapore (.sg) domain name disputes.[76]

In 2004, the Philippines launched an ODR that was hailed as "one of the most technologically impressive of the new ODR websites". The founders of the service anticipated that it would become a web-based multi-door courthouse offering several services: "Neutral evaluation, for an unbiased assessment of the case by a neutral expert; mediation, for assistance in forging a settlement; arbitration, for a binding ruling of the case; and blind bidding, an automated bidding program that allows parties to a purely monetary dispute to identify the optimal settlement amount." Also, in 2004, Malaysia launched ODRWorld to help people looking to get what is rightly owed to them, even in the case of negligible sums or non-monetary transactions.

The 21 economies of the Asia Pacific Economic Cooperation (APEC) group established a work programme on Online Dispute Resolution in 2017. To date, this has consisted of sharing experiences. During their meeting in 2018, APEC Ministers Responsible for Trade underscored the importance of developing a cooperative online dispute-resolution framework for micro and small and medium enterprises. The topic has also risen in prominence on the ASEAN agenda.

In Mexico, Concilianet is a free online platform for resolving disputes between merchants and customers, which has reduced the time for resolving disputes by 50% and led to settlements in almost 96% of cases filed through its platform. Brazil established an online negotiation platform called Consumidor.gov.br in June 2014. By the end of 2016, the platform had already handled more than 560,000 complaints concerning suppliers of goods and services and the majority had been resolved before lawsuits were undertaken. Complaints were mainly filed against merchants in the telecommunications sector (47.5%), banks (23.9%) and a minority of companies in the e-commerce segment (9.7%).[77]

ODR in Africa has lagged due to uneven internet access. It has been more prominent in South Africa where e-commerce use is higher. The country currently has two ODR programmes – the ZA Domain Name Dispute Resolution Regulations (ZADRR) and the Online Ombudsman.

When disputes arise in cross-border e-commerce, business and consumers need to be certain about what rules are applicable, and how to reach a solution for the issue. A proposition to legally locate all consumer disputes in the jurisdiction of the consumer was presented by the Canadian and Brazilian delegations to the Organization of American States (OAS) in 2009, but it met with significant resistance.[78]

Consequently, the US State Department offered a blueprint for a global ODR system for resolving consumer disputes that would not be reliant on "home-state" jurisdiction. The proposal initially met with enthusiasm. An UNCITRAL group took up the topic, meeting biannually from 2010 to 2016. Discussion focused on establishing global ODR procedures for small-value B2C transactions as well as B2B disputes from internet transactions.

Differences emerged, however, around the inclusion of binding arbitration procedures. Consensus remained out of reach and the group's mandate ran short. [79] Ultimately, the group did not denounce ODR, but, instead, encouraged nations to consider more forward-thinking ODR systems.

Acknowledgements

The authors would like to thank Arlyn Wiener for her wonderful research assistance and Meg Cochrane for excellent editorial assistance and comments. Thanks and recognition for review are also extended to the following individuals: Justin Macmullan, Advocacy Director, Consumers International; Eduardo Pedrosa, Secretary General, Pacific Economic Cooperation Council (PECC); François Martins, Head Government Relations, Mercado Libre Brazil; Ricardo Dalmaso Marques, Dispute Resolution Senior Manager, Mercado Libre Brazil; Akira Yoshida, Policy Analyst, Organisation for Economic Cooperation and Development (OECD); Martín Molinuevo, Senior Counsel, World Bank Group; Ujjwal Kumar, Policy Analyst, CUTS International, Jaipur; Amol Kulkarni, Fellow, CUTS International; Mark Wu, Stimson Professor of Law, Harvard Law School, USA, and special thanks to Kimberley Botwright, Community Lead, International Trade and Investment, World Economic Forum, who has significantly contributed to the framing and editing of this paper.

Endnotes

1 For some stakeholders, "e-commerce" refers to the online sale of goods and services. The OECD offers a broader definition of "…the sale or purchase of goods and services conducted over computer networks by methods specifically designed for the purpose of receiving or placing orders", even if the payment and the ultimate delivery of the goods and services are not conducted online. See https://stats.oecd.org/glossary/detail.asp?ID=4721 (link as of 6/3/19).

2 Despite its growing significance, e-commerce has developed unevenly across different jurisdictions. For example, it accounts for 13% of consumer spending in the US, around 10% in Europe – though significantly more in the UK and Germany – but it represents a low percentage of consumer spending in Africa (Source: International Trade Centre, "Bringing SMEs onto the E-commerce Highway", 2016). The reasons vary and include poor connectivity, limited digital skills, payment and logistical issues, language barriers, cultural preferences and so on.

3 https://unctad.org/en/PublicationsLibrary/ier2017_en.pdf (link as of 6/3/19).

4 Several studies highlight the importance of consumer trust in e-commerce. These studies focus on both issues of security (e.g. encryption) of the communications and the information exchanged as well as on privacy and other dimensions related to the quality of service. The latter are less likely to be resolved with the application of technical solutions but require the institution of a socioeconomic and legal framework that specifically promotes and protects trust in e-commerce.

5 F. Kamari and S. Kamari, "Trust in Electronic Commerce: A New Model for Building Online Trust in B2C", European Journal of Business and Management, 10(4), 2012, 125.

6 The issue is not solely limited to online transactions though, since it is possible that information given offline may eventually be leaked online: https://www.pecc.org/resources/trade-and-investment-1/2201-regulating-data-a-korean-perspective/file (link as of 6/3/19).

7 Although it has been reported that consumers are unwilling to approach formal grievance redress systems: https://www.centerforfinancialinclusion.org/lessons-from-running-a-consumer-care-center-in-india/ (link as of 6/3/19).

8 Julie Hunter and Dr. Christine Riefa, "The Challenge of Protecting EU Consumers in Global Online Markets", European Consumer Organisation (BEUC) and the Federation of German Consumer Organisations, November 2017.

9 See 2017 CIGI-Ipsos Global Survey on Internet Security and Trust: https://www.cigionline.org/internet-survey-2017 (link as of 7/3/19).

10 See European Commission, Consumer Conditions Scoreboard (2015): https://ec.europa.eu/info/publications/consumer-conditions-scoreboard-consumers-home-single-market-2015-edition_en (link as of 6/3/19).

11 There is a lot of literature on the existence of significant differences in depersonalized trust (i.e. trust towards a relatively unknown target person) across cultures, finding that trust influences not so much how we trust, but the way we trust. See E. Krockow, A. Colman and B. Pulford, "Are Some Cultures Less Trusting Than Others?", The Conversation, 2018, which refers to research by T. Yamagishi and M. Yamagishi, "Trust and Commitment in the United States and Japan", Motivation and Emotion, 18(2), 1994, 129, which differentiates between two different types of trust. The first is "general trust", which denotes "spontaneous trust towards strangers" and is prevalent in individualistic Western cultures. The second is "assurance-based trust", which denotes "a more reciprocal type of trust towards people already previously encountered" and characterizes Asian cultures. This has implications for the relationship between trust and e-commerce, as contrary to traditional commerce, which often relies on assurance-based trust, e-commerce mostly requires high levels of general trust.

12 International Trade Centre (2), 49–50.

13 The list of international bodies having touched on the subject to date include, among others, the United Nations (UN), World Trade Organization (WTO), World Bank, the European Union, the Asia Pacific Economic Cooperation (APEC), the Organisation for Economic Cooperation and Development (OECD) and the Association of Southeast Asian Nations (ASEAN).

14 OECD, "Consumer Protection Enforcement in a Global Digital Marketplace", OECD Digital Economy Papers, No. 266, 2018, OECD Publishing, Paris: https://doi.org/10.1787/f041eead-en (link as of 6/3/19).

15 Issues related to digital competition are noted in as far as they affect consumer trust and bargaining power – but are not the primary topic of the discussion, which merits close examination.

16 The International Consumer Protection and Enforcement Network and its members share information about cross-border commercial activities that may affect consumers' interests and encourage global cooperation among law enforcement agencies.

17 Consumers International is a global federation of consumer groups. It consists of more than 250 organizations from 120 countries, with five main offices on different continents. It was established in 1960, just as consumer law and policy began to develop.

18 United Nations Conference on Trade and Development (UNCTAD), "Summary of Adoption of E-Commerce Legislation Worldwide" (unctad.org): https://unctad.org/en/Pages/DTL/STI_and_ICTs/ICT4D-Legislation/eCom-Global-Legislation.aspx (link as of 6/3/19).

19 International Trade Centre (2), 50.

20 H. Ha and S. McGregor, "Role of Consumer Associations in the Governance of e-Commerce Consumer Protection", Journal of Internet Commerce, 12(1), 2013,1.

21 International Trade Centre (2).

22 KPMG, "The Trust About Online Consumers – 2017 Global Online Consumer Report" (2017): https://assets.kpmg.com/content/dam/kpmg/xx/pdf/2017/01/the-truth-about-online-consumers.pdf (link as of 6/3/19).

23 S. Barth and M. D. T. de Jong, "The Privacy Paradox: Investigating Discrepancies Between Expressed Privacy Concerns and Actual Online Behavior – A Systematic Literature Review", Telematics and Informatics, 34(7), 2017, 1038.

24 Acquisti et al. suggest that consumers often prefer short-term discounts over the long-term risk of disclosing personal information. L. K. John and G. Loewenstein, "What Is Privacy Worth?", The Journal of Legal Studies, 42(2), 2013, 249–74; and A. Acquisti, C. Taylor and L. Wagman, "The Economics of Privacy", Journal of Economic Literature, 54(2), 2016, 442–92.

25 See, for instance, the meta-study by J. Mou, D.-H. Shin and J. Cohen, "Trust and Risk in Consumer Acceptance of E-Services", Electronic Commerce Research, 17(2), 2017, 255. A recent CUTS International survey on privacy and data protection in India covering 2,400 respondents revealed that around 80% of users were not reading privacy policies. The main reasons were policies being lengthy, the language barrier and too much legalese: http://www.cuts-ccier.org/pdf/Advocacy-CUTS_Comments_on_the_draft_Personal_Data_Protection_Bill2018.pdf (link as of 6/3/19).

26 See G Contissa et al., "Towards Consumer-Empowering Artificial Intelligence, Proceedings of the 27th International Joint Conference on Artificial Intelligence Evolution of the Contours of AI", pp. 5150–7: https://doi.org/10.24963/ijcai.2018/714 (link as of 6/3/19).

27 Some have coined the term "algorithmic consumer" to convey the complexity of the decision process in the digital era of the internet of things: M. Gal and N. Elkin-Koren, "Algorithmic Consumers", Harvard Journal of Law and Technology, 30, 2017: https://ssrn.com/abstract=2876201 (link as of 6/3/19).

28 General Data Protection Regulation (EU) 2016/679, the protection of natural persons regarding the processing of personal data and on the free movement of such data [2016] OJ L 119/1.

29 See, for instance, the California Consumer Privacy Act of 2018 in the US, the Personal Data Protection Bill 2018 in India and the Brazilian General Data Protection Law of 2018.

30 Christoph Busch, "European Model Rules for Online Intermediary Platforms". In U. Blaurock, N. Schmidt-Kessel and K. Erler (eds), Plattformen – Geschäftsmodelle und Verträge, Nomos, 2018, 37

31 E-Commerce Law of the People's Republic of China (adopted 31 August 2018, effective 1 January 2019), Chapter II, Section 2.

32 OECD, "Industry Self-Regulation: Role and Use in Supporting Consumer Interests", 2015: http://www.oecd.org/å/publicdisplaydocumentpdf/?cote=DSTI/CP(2014)4/FINAL&docLanguage=En (link as of 6/3/19).

33 The Transatlantic Consumer Dialogue recently defined co-regulation as "self-regulation operating within a legislative framework so that there is a legal backup available to consumers where a voluntary scheme fails".

34 UN General Assembly, A/RES/*39/248* on Consumer Protection.

35 http://www.oecd.org/going-digital/topics/digital-consumers/ (link as of 3/6/19).

36 http://www.oecd.org/sti/consumer/online-advertising-roundtable-summary.pdf (link as of 6/3/19).

37 https://www.oecd-ilibrary.org/science-and-technology/protecting-consumers-in-peer-platform-markets_5jlwvz39m1zw-en;jsessionid=iK0yjWvppjEQvfEqiIKuvATM.ip-10-240-5-171 (link as of 6/3/19).

38 For example, in 2003, the OECD produced Guidelines for Protecting Consumers from Fraudulent and Deceptive Commercial Practices Across Borders, and in 2006 OECD members also approved a Recommendation on Cross-border Cooperation in the Enforcement Laws Against Spam.

39 "G20 Consumer Summit: Building a Digital World That Consumers Can Trust", 2017: https://www.bmjv.de/G20/EN/ConsumerSummit/G20_node.html (accessed 22 January 2019) (link as of 6/3/19).

40 See WTO General Council, "WTO Agreements and E-Commerce" (WT/GC/W/90), 1998, 2; M. Wu, "Digital Trade-Related Provisions in Regional Trade Agreements: Existing Models and Lessons for the Multilateral Trading System", Report for International Centre for Trade and Sustainable Development, 2017, 2–3.

41 See WTO Panel, "United States – Measures Affecting the Cross-Border Supply of Gambling and Betting Services", Report WT/DS285/R, 2005, which concerned online gambling and betting services; WTO Panel, "China – Measures Affecting Trading Rights and Distribution Services for Certain Publications and Audio-Visual Entertainment Products", Report WT/DS363/R, 2010, which concerned electronic distribution services. Note that the GATS provides for general (e.g. MFN and transparency) and specific (e.g. market access and national treatment) disciplines; the latter applies only to the extent that a WTO member has undertaken specific commitments in its GATS schedule.

42 WTO Ministerial Conference, "Declaration on Global Electronic Commerce", 2nd Session, 1998 (WT/MIN(98)/DEC/2), [2]. On that occasion, ministers also agreed to continue, for the next two years, their practice of not imposing customs duties on electronic transmissions, and this moratorium has been renewed at each WTO Ministerial Conference since then – most recently, WTO Ministerial Conference, "Work Programme on Electronic Commerce – Ministerial Decision of 13 December 2017", 11th Session (WT/MIN(17)/65), [2].

43 WTO Ministerial Conference, "Joint Statement on Electronic Commerce", 11th Session Statement, 2017 (WT/MIN(17)/60). Note that the EU and its member states constituted 29 of the 70 signatories.

44 "The Consumer Checklist for an International E-commerce Deal". Consumers International: https://www.consumersinternational.org/media/155222/consumerchecklistforinternationale-commercedeal.pdf (accessed 22 January 2019) (link as of 6/3/19).

45 The Appellate Body is the WTO's highest court of appeal. Seven Appellate Body members are appointed by WTO members. In recent years, however, the United States has been blocking appointments and reappointments due to frustrations expressed with the dispute system. The WTO's legal agreements require at least three Appellate Body members to serve on cases and these are selected by rotation. As of October 2018, only three Appellate Body members remained, rendering the rotation meaningless and the workload crippling. The terms of the US and Indian members will be up in December 2019. A crisis in the WTO's dispute settlement system, or at least in the appeals process, is expected at that point should no agreement on reform be reached between WTO members before then.

46 See Article 2.4 of the TBT Agreement and Article 3 of the SPS Agreement. In the latter case, the competent international organizations are Codex Alimentarius Commission with respect to food safety, the World Organisation for Animal Health, and the Secretariat of the International Plant Protection Convention (IPPC) in the area of plant health (Annex A.3).

47 See Article 2.7 of the TBT Agreement and Article 4 of the SPS Agreement.

48 These concern regulatory principles in interconnection, universal service, licensing, allocation and use of scarce resources. See, WTO, "Negotiating on Basic Telecommunications", Reference Paper, 1996.

49 WTO Dispute Settlement System: Article 3, "Understanding on Rules and Procedures Governing the Settlement of Disputes (DSU)".

50 See WTO Secretariat, "Provisions on Electronic Commerce in Regional Trade Agreements", WTO Working Paper ERSD-2017-11, 6–7; Wu (49), 6–7.

51 WTO Secretariat, 14.

52 Ibid.

53 Ibid, 24.

54 See Ibid, 48; Organisation for Economic Co-operation and Development (OECD), "Consumer Protection in E-Commerce", Recommendation, Principle F, 2016.

55 For a more detailed discussion, see WTO Secretariat (63), 51–3; and Wu (49), 20–1.

56 E.g. "Australia–Singapore Free Trade Agreement", Chapter 12, Article 9.2, 2003: "Each party shall adopt or maintain a legal framework that provides for the protection of the personal information of the users of electronic commerce. In the development of its legal framework for the protection of personal information, each party should take into account principles and guidelines of relevant international bodies"; "Australia–Japan Economic Partnership Agreement", Article 13.5, 2015; "China–Korea Free Trade Agreement", Article 13.5, 2014; "New Zealand–Thailand Closer Economic Partnership Agreement", Article 13.5, 2005; and "Additional Protocol to the Framework of the Pacific Alliance", Article 13.8, 2014.

57 For a more detailed discussion, see WTO Secretariat (63), 46–9; Wu (49), 19–20.

58 E.g. “Japan–Switzerland Free Trade and Economic Partnership Agreement”, Article 80.1, 2009, whereby “the parties recognize the importance of adopting and maintaining transparent and effective consumer protection measures for electronic commerce as well as measures conducive to the development of consumer confidence”. One exception is the “Australia–Singapore Free Trade Agreement”, Chapter 14, Article 8.3: “Each party shall adopt or maintain consumer protection laws to proscribe fraudulent and deceptive commercial activities that cause harm or potential harm to consumers engaged in online commercial activities.”

59 E.g. “Australia–China Free Trade Agreement”, Chapter 12, Article 12.7, 2015: “Each party shall, to the extent possible and in a manner it considers appropriate, provide protection for consumers using electronic commerce that is at least equivalent to that provided for consumers of other forms of commerce under their respective laws, regulations and policies.”

60 For a more detailed discussion, see WTO Secretariat (63), 54–6; Wu (49), 21–2.

61 E.g. “Additional Protocol to the Framework of the Pacific Alliance”, Chapter 13, Article 13.9, 2014: “Each party shall adopt or maintain measures to protect users from unsolicited commercial electronic messages.” The most advanced set of binding commitments on this issue is found in the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP), the modified Trans-Pacific Partnership (TPP): see Wu (49), 22.

62 Wu, 2.

63 Such regulatory convergence seems thus far to be limited in most of the e-commerce-related disciplines under RTAs: Ibid, 28–9.

64 Aaditya Mattoo and Joshua Paul Meltzer, “International Data Flows and Privacy: The Conflict and Its Resolution (English)”, Policy Research Working Paper No. WPS 8431, 2018, Washington, D.C: World Bank Group.

65 ASEAN Secretariat, “E-ASEAN Reference Framework for Electronic Commerce Legal Infrastructure”, 2001.

66 The ASEAN Strategic Action Plan for Consumer Protection (ASAPCP) identifies four goals for the period 2016–2025: Establish a common ASEAN consumer protection framework; ensure a high common level of consumer empowerment; establish high consumer confidence across the region; integrate consumer concerns in all ASEAN policies.

67 https://asean.org/storage/2012/05/ASAPCP-UPLOADING-11Nov16-Final.pdf (link as of 6/3/19).

68 Competition and Markets Authority (CMA), “Online Hotel Booking” (gov.uk, 27 October 2017): https://www.gov.uk/cma-cases/online-hotel-booking (link as of 6/3/19).

69 Canada’s Anti-Spam Law, Art. 12 (1).

70 Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market and amending Council Directive 84/450/EEC, Directives 97/7/EC, 98/27/EC and 2002/65/EC of the European Parliament and of the Council and Regulation (EC) No 2006/2004 of the European Parliament and of the Council (“Unfair Commercial Practices Directive”) (OJ L 149, 11.6.2005, p. 22–39), Arts. 2 (b) and 3.

71 Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the internal market (“Directive on Electronic Commerce”) (L 178, 17/07/2000 p. 0001 – 0016), Art. 14. Brazilian law adopts a similar approach.

72 Proposal for a Directive of the European Parliament and of the Council amending Council Directive 93/13/EEC of 5 April 1993, Directive 98/6/EC of the European Parliament and of the Council, Directive 2005/29/EC of the European Parliament and of the Council and Directive 2011/83/EU of the European Parliament and of the Council as regards Better Enforcement and Modernization of EU Consumer Protection Rules, COM/2018/0185 final.

73 It has been reported that South Korea is overhauling its law on consumer protection in e-commerce: http://www.koreaherald.com/view.php?ud=20181203000466 (link as of 6/3/19).

74 Directive 98/6/EC of the European Parliament and of the Council of 16 February 1998 on Consumer Protection in the Indication of the Prices of Products Offered to Consumers [1998], L 80/27.

75 Colin Rule, “Asia: The New Frontier for Online Dispute Resolution”, ACRESOLUTION 34, Spring 2005: https://www.mediate.com/Integrating/docs/34worldviews.pdf (link as of 6/3/19).

76 Online shopping platform Mercado Libre in Mexico uses the Concilianet programme for 0.06% of claims that remain unresolved on the company’s own ODR platform. Of those treated on Concilianet, Mercado Libre reported a 90% solution rate. The company joined Brazil’s Consumidor platform in 2017 and has since solved 99.2% of its users’ claims out of court.

77 Colin Rule et al., “Designing a Global Consumer Online Dispute Resolution (ODR) System for Cross-Border Small Value-High Volume Claims—OAS Developments”, Uniform Commercial Code Law Journal, 42(3), 2010, 221, 222–50.

78 https://documents-dds-ny.un.org/doc/UNDOC/GEN/V16/014/73/PDF/V1601473.pdf?OpenElement (link as of 6/3/19).

WORLD ECONOMIC FORUM

COMMITTED TO IMPROVING THE STATE OF THE WORLD

The World Economic Forum, committed to improving the state of the world, is the International Organization for Public-Private Cooperation.

The Forum engages the foremost political, business and other leaders of society to shape global, regional and industry agendas.

World Economic Forum
91–93 route de la Capite
CH-1223 Cologny/Geneva
Switzerland

Tel.: +41 (0) 22 869 1212
Fax: +41 (0) 22 786 2744

contact@weforum.org
www.weforum.org