BEUC The European Consumer Organisation

The Consumer Voice in Europe

Putting consumer interests at the heart of the EU's global digital leadership

BEUC's input to the European Commission's call for evidence for the Joint Communication on an International Digital Strategy

Contact: Mykyta Sobko – international@beuc.eu

BUREAU EUROPÉEN DES UNIONS DE CONSOMMATEURS AISBL | DER EUROPÄISCHE VERBRAUCHERVERBAND
Rue d'Arlon 80, B-1040 Brussels • Tel. +32 (0)2 743 15 90 • www.twitter.com/beuc • www.beuc.eu
EC register for interest representatives: identification number 9505781573-45

Co-funded by the European Union

Ref: BEUC-X-2025-048 - 19/05/2025

Why it matters to consumers

Every day, EU consumers shop and engage with services online, including those provided by non-EU companies. However, engaging with these companies can expose them to a range of risks, including unlawful personal data processing and transfers and unfair AI systems for consumer use. Recent EU trade agreements have begun to address this issue through digital trade provisions or standalone Digital Trade Agreements, which is a positive development. However, the EU is also including other rules in its trade agreements on cross-border data flows and access to source code, which could undermine consumer privacy and limit regulatory oversight of algorithmic systems.

1. Introduction

The recent proliferation of digital trade agreements, the potential integration of the Joint Statement Initiative (JSI) on e-commerce into the World Trade Organisation framework, and other forms of international digital cooperation reflect the EU's ambition to become a global standard-setter. While these initiatives aim to strengthen consumer trust in the digital economy by improving access to information and enhancing redress mechanisms, some fall short of established EU standards and could negatively impact the ability of the EU to apply or enforce its digital laws. In the current context of the global technological race, it is crucial that the EU advances its strategic interests in digital transformation with consumer protection at its core.

2. Digital trade: how to get it right for consumers?

Consumers are facing similar challenges across the globe when going online. They can be scammed, their personal data can be misused, and they can enjoy less options if artificial intelligence (AI) systems are not designed properly. Getting digital trade right for consumers means fostering international cooperation that upholds high consumer protection standards. In fact, consumers could be better protected if EU and foreign authorities would cooperate more and exchange data of their respective investigations while preserving due process. Flexible, non-binding frameworks allow regulators to exchange best practices, respond to emerging risks, and adapt to technological developments, particularly in sensitive areas such as data protection, online safety, and AI governance. We would like to raise awareness about the unintended consequences of recent rules in digital trade agreements. Indeed, prematurely codifying detailed digital trade commitments in binding agreements risks constraining the EU's ability to strengthen consumer safeguards as challenges evolve.

2.1. Data flows, data protection and privacy

Cross-border data flow provisions have become a standard feature of digital trade negotiations, often driven by corporate interests seeking unrestricted data transfers. But personal data isn't a tradable asset, it's tied to people's privacy and personal data rights. The EU already has a strong tool for enabling digital trade without lowering standards: adequacy decisions and other data transfer mechanisms under the GDPR. Where these are not an option, the EU's 2018 agreement between the Parliament, Council and Commission sets out a clear condition: data flow rules in trade deals should not limit the EU's ability or ambition to protect personal data.

Unfortunately, in some recently concluded agreements, the European Commission seems to be moving beyond that mandate. By adjusting the EU's data flow clauses to fit the interests of trading partners, it risks creating legal uncertainty and weakening consumer safeguards. The recent €530 million fine against TikTok for illegally transferring EU users' data, including minors', to China is a stark reminder of what's at stake. If the EU wants to lead globally on digital policy, it is paramount to stay true to its own commitments and keep privacy and data protection at the core of its international strategy.

2.2. Prohibition on access to source code

Foreign countries sometimes ask EU companies to provide access to their software source code to obtain a licence to operate in their markets. This tends to lead to intellectual property theft. To better protect companies, the EU agreed in recent years with several trading partners to ban this practice in this agreement. We're concerned that the way this provision has been drafted may limit regulatory bodies' ability to ensure that companies comply with laws such as the AI Act. Without easy access to source code, investigations into fraudulent practices and security vulnerabilities could be obstructed, compromising consumer safety and trust, as in the Volkswagen emissions scandal. Companies already have protections for their intellectual property and trade secrets. This new layer of protection for companies could come at the expense of the enforcement of EU law and is therefore not proportionate to the intended goal. This being said, consumers, however, would benefit from closer cooperation between the EU and third countries on AI. This could be an interesting angle to further develop in the strategy.

2.3. Shaping responsible digital trade policy

As the EU continues negotiating digital trade agreements with countries like Indonesia, the Philippines, Thailand, and Malaysia, there is still time to secure benefits for consumers. It is paramount that future deals fully align with EU laws and leave space for policy developments. This means avoiding commitments on issues like source code access, unless strong safeguards are included, as seen in the EU-New Zealand free trade agreement. When it comes to data flows, the EU should stick to its 2018 model clause or rely on tools like adequacy decisions. Where possible, flexible cooperation formats like digital partnerships or memoranda of understanding should be preferred over binding trade rules. This approach would help protect consumer rights while supporting innovation and digital cooperation globally.

3. Enforcing the EU's digital laws, despite external pressures

The EU's digital laws, such as the Digital Markets Act and the Digital Services Act, are essential to making online markets safer, more competitive, and fairer for consumers. These rules help rein in the power of dominant tech companies and ensure people have more choice and protection online. As enforcement begins, the EU is facing growing geopolitical pressure. The recent reaction from the United States, threatening trade retaliation over EU digital rules, shows how global tech lobbying can challenge democratic decision-making. The EU must stay the course and uphold the laws agreed by its democratic institutions. Strong enforcement and respect for the rule of law are essential to safeguarding consumer rights and upholding the EU's global leadership in digital policy. Achieving this requires better coordination among enforcement authorities across areas such as consumer protection, digital regulation and competition policy.

Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or EISMEA. Neither the European Union nor the granting authority can be held responsible for them.