



The below are comments to the European Commission on the potential Digital Services Act (DSA), the current framework for regulating e-commerce platforms, and the proposal for Know Your Business Customer (KYBC) requirements to be included in the DSA.

### ***The E-Commerce Directive as a 20<sup>th</sup> Century Solution to Modern Problems***

At the time the E-Commerce Directive (ECD) was adopted, it was motivated primarily by the potential of e-commerce. The Directive aimed to create an online marketplace that created “closer links between the States and peoples of Europe, to ensure economic and social progress,” and that provided “significant employment opportunities to the community.” (Council Directive 2000/31/EC). While the potential of e-commerce was known to all, online businesses were relatively small, with many of today’s most prominent businesses yet to be founded.

This concern with potential led the ECD to focus on bolstering and protecting the development of online platforms. Since fostering the potential of this sector was viewed as paramount, the ECD sought to spur the growth of these new businesses by relieving them of responsibilities borne by offline businesses. It was believed that the growth of online platforms would be impeded if the law imposed duties to monitor and remedy harms caused by customers and business partners. The operational and technical challenges at the time were asserted to be too daunting and costly for this young industry.

Following the lead of U.S. legislation, the ECD created a framework that relied on self-regulation coupled with a liability shield. Rather than imposing responsibility, the ECD cleared a path for online businesses, largely by relieving them of responsibilities required of offline competitors.

This approach yielded robust results, although perhaps not exactly the results originally intended or anticipated. On the one hand, innovation flourished, and the citizens of the EU, and the world, now enjoy a vast digital marketplace. On the other hand, the rules shaped the types of businesses that flourished online, opening a path for businesses that followed the opportunities created by liability shields and limited responsibilities. As a result, the online marketplace is dominated by a few very large, wealthy, and powerful companies, which often thrive by serving as a platform for third parties to communicate and sell goods and services. Some of this result was shaped by the nature of the medium, but some of it was shaped by regulation, or lack thereof.

Being an online platform for the publication and sales of third parties demands fewer responsibilities and incurs fewer liabilities than publishing or selling on one’s own behalf online. E-commerce is thus dominated by those who facilitate communication and sales of goods and services by others, rather than selling or communicating on their own behalf, from eBay and Yahoo in the 90s to Uber, AirBnB, and Twitter in more recent years. While these online platforms provide desirable services, they often avoid the obligations that an offline business

would have to protect consumers; respect labor, housing, or other regulations; provide recourse to other businesses and consumers suffering fraud or other injury inflicted by sellers; or even simply to help other businesses and consumers find and hold accountable those who use their platforms to communicate or sell goods.

The ECD's late-20<sup>th</sup> Century assumptions and methods grow more inappropriate every year. Its framework is designed to shield and foster infant industries. The infant businesses of the turn of the century are now the world's wealthiest, most powerful, and technologically adept businesses. They no longer need special protection, and society no longer benefits from it.

In recent years, the EU has recognized the need to ask more of online businesses. Recent reforms have required them to take greater responsibility for their actions, benefitting consumers and leveling the playing field with offline businesses. Thus, recent years have brought more uniform and transparent rules for data protection (the 2017 [General Data Protection Regulation](#)); more responsibility for platforms regarding what they do with copyright owners' creations (the 2019 [Copyright Directive](#)); and greater accountability regarding platform-to-business practices (2019 [Regulation on promoting fairness and transparency for business users of online intermediation services](#)).

The DSA is an opportunity to continue this trend toward greater transparency and accountability, correcting the unintended consequences of exempting online businesses from the responsibilities and accountability imposed on other businesses.

### ***Creating a 21<sup>st</sup> Century Regulatory Framework for E-commerce***

In February of 2020 the Commission recognized that it was time for a 21<sup>st</sup> Century regulatory framework and launched the "Shaping Europe's digital future" initiative. This initiative had three main pillars, the second of which was to create a fair and competitive digital economy. The initiative aims to build this pillar by, among other things, "strengthen[ing] the responsibility of online platforms by proposing a Digital Services Act."

We agree that strengthening the responsibility of online platforms is a key component of reforming and modernising the regulatory framework for e-commerce in the EU, and suggest that the following principles will help achieve this responsibility:

- **A Level Playing Field.** Online and offline businesses should be subject to the same obligations and legal liabilities. Online regulation should follow the fundamental principle that "what is illegal offline is also illegal online."
- **A Fair and Safe Online Environment.** Online business models should not be founded on opportunities created by liability shields and regulatory gaps. Rather, online

businesses should be required to deal fairly with and respect the rights of consumers and other businesses, just as they would offline.

- **A Free and Efficient Marketplace.** Regulation should preserve the free movement of digital services and a free marketplace. It should take account of the particular circumstances of online businesses. However, preserving a free and efficient market does not require excusing online platforms from responsibility, but rather the same common sense regulation to which offline businesses are subjected.

The principles we recommend here largely echo those proposed in the Draft Lead Report of the Internal Market and Consumer Protection Committee (IMCO), “[Digital Services Act: Improving the functioning of the Single Market](#),” specifically:

The Digital Services Act should contribute to the strengthening of the internal market by ensuring the free movement of digital services *and the freedom to conduct a business*, while at the same time guaranteeing a high level of consumer protection, *and the improvement of users’ rights, trust and safety online*.

The Digital Services Act should guarantee that online and offline economic activities are treated equally and on a level playing field, which fully reflects the principle *according to which* “what is illegal offline is also illegal online”, *taking into account the specific nature of the online environment*.

These principles are neither novel nor particularly onerous. The exemption of online businesses from the rules imposed on all other businesses represents a tremendous deviation from the norm. Asking online businesses to play by the same rules as others

only seems remarkable because they have built large, vastly profitable businesses on the foundation of their exemption from the rules.

The current self-regulatory/liability shield regime does not, and cannot, serve these principles. While recent regulatory reforms and some court decisions have imposed more responsibilities on online businesses, the current regime leaves a vast “regulatory gap” that courts and member states cannot close. This gap is well-documented in one of the supporting studies commissioned by the IMCO. (Smith, M. [Enforcement and cooperation between Member States in a Digital Services Act](#), Study for the Committee on Internal Market, Policy Department A for Economic, Scientific and Quality of Life Policies, European Parliament, Luxembourg, 2020.)

As that report says, “the last 20 years have shown that there is no incentive to comply. If a new DSA is to have any purpose, then enforceability of rules should be a priority for legislators.”

There are several laudable proposals being considered that would lead to enforceable rules in accordance with the principles we have advocated. We write here in support of one in particular, which we believe would contribute to a level playing field and a fair and safe online environment while supporting and enhancing a free and efficient marketplace: The Know Your Business Customer Principle.

### **The “Know Your Business Customer” Principle**

The “Know Your Business Customer” (KYBC) principle is directed towards reinforcing and improving the information and transparency requirements of Articles 5, 6 and 10 of the E-Commerce Directive. It would require online businesses to verify and retain information regarding the businesses with which they are dealing. Simply put, KYBC would require online platforms to verify the identity of sellers and other business customers so that other businesses and consumers could find and get a remedy from platform users who harm them. This requirement would create a more level playing field between online and offline businesses while fostering a safer and fairer online environment.

KYBC would level the playing field between online and offline businesses by imposing on them practices widely followed in the business world as either (or both) a matter of best practice or regulation. In many contexts, offline businesses find it in their best interest to know who their customers are, perhaps more so than online businesses, because physical resources can be wasted, lost, or damaged where digital ones are less vulnerable and scarce. Thus, for example, a commercial landlord will need to know who its tenants are and how to reach them, whereas an online business may not be as concerned.

Even where offline businesses might find it useful, or profitable, not to ask too many questions of their business customers, the law often intervenes to protect consumers and society. Thus, a physical market owner may find itself liable if it tolerates or harbors fraudulent sellers. Also, and in particular, the financial industry has increasingly been regulated with the imposition of Know Your Customer (KYC) requirements.

In Europe, KYC requirements have become a familiar and important part of the regulatory landscape, imposed to combat money laundering and increase transparency in the wake of the Global Financial Crisis in 2007. Several regulations, including the Fourth, Fifth & Sixth Anti-Money Laundering Directives and the Payment Services Directive, have sought to make it easier to identify customers, to trace wrongdoing, and have developed standards for authenticating identity. (Know Your Customer, [European KYC regulations and their impact on the compliance function](#)). Best practice KYC requires financial institutions to know their customer’s identity, understand the nature of the customer’s activities, and assess money laundering risks associated with that customer for purposes of monitoring the customer’s activities.

One of the functions of KYC regulations in the financial sector was both to protect the public and to restore public trust in financial institutions. First the Financial Crisis, and then a series of money laundering scandals, notably the Panama Papers, caused the public to question the integrity of the system. The implementation of KYC regulations on financial institutions helped address the public's distrust. Greater transparency in the financial marketplace was aimed to regain the trust of customers.

Just as financial institutions faced public concern in 2007 and the years afterward, the public's attitude toward digital service providers is becoming skeptical. Online counterfeits and other forms of fraud are perceived as rampant, particularly with respect to scams related to the current COVID-19 pandemic. (Know Your Customer, [European KYC regulations and their impact on the compliance function](#)) Dishonest traders selling fake or illegal personal protective equipment or false remedies undermine confidence in the system. Even more troublesome is that fact that the identity of the fake traders often cannot be established, despite the current requirements of Article 5 to clearly identify sellers. Online platforms lend their legitimacy to sellers and advertisers, but are under no obligation currently to ensure that these customers are who they say they are. The implementation of a KYBC model would update the law to advance the first goal of the E-Commerce directive, by encouraging economic and social progress through transparency

and keeping service providers accountable for their users by requiring them to know their business customer.

Finally, a KYBC requirement can and should meet the principle of making the digital marketplace more efficient and freer. Information requirements should be standardized, and, at least initially, pre-existing sources of identification, such as the EU VAT and Economic Operator Identification and Registration databases. In the long run, it would be useful to develop standards for portable, global, and user-owned digital credentials, using blockchain or other technology. A KYBC requirement need not be onerous in its implementation, and with proper care, requirements can increase efficiency and transparency in the marketplace.

In conclusion, a KYBC requirement should be included in the DSA as a modest, but significant reform toward bringing EU e-commerce regulation into the 21<sup>st</sup> Century. If done properly, it can meet key goals of leveling the playing field between online and offline businesses, ensuring a fair and safe online marketplace, and making e-commerce more transparent and efficient.