DIGITAL SERVICES ACT PACKAGE: OPEN PUBLIC CONSULTATION

SIDE PAPER TO IBM'S RESPONSE TO THE EUROPEAN COMMISSION

8 SEPTEMBER 2020

IBM is the largest technology and consulting employer in the world, serving clients in 175 countries. Today, 47 of the Fortune 50 companies rely on the IBM Cloud to run their business and IBM Watson enterprise AI is deployed in more than 20,000 engagements. IBM is one of the world's most vital corporate research organizations, with 26 consecutive years of patent leadership.

With more than 100 years of commitment in Europe, IBM is one of the largest technology employers in the EU and has many cloud data centers, research labs, innovation spaces, centers of excellence, etc. spread across Europe. IBM scientists from 50+ nationalities work in Europe on cutting-edge research and IBM will build Europe's first quantum computer in Germany.

IBM's expertise is in the intersection of technology and business, providing artificial intelligence (AI) and cloud-based solutions that are changing the way the world works. Above all, guided by principles for trust and transparency and support for a more inclusive society, IBM is committed to being a responsible technology innovator and a force for good in the world. For more information, visit www.ibm.com.

INTRODUCTION

IBM welcomes the opportunity to contribute to the European Commission's consultation on the Digital Services Act (DSA) package, and to offer our views on the measures we believe can help frame the responsibilities of digital services to address the risks faced by online users and protect their rights. We also welcome the opportunity to share our thoughts on how to ensure that all digital services can compete fairly in the Digital Single Market where both consumers and businesses can benefit from the widest choice.

IBM is a business-to-business (B2B) technology company with a large and diverse portfolio of products and services. Those offerings include cloud computing, AI, data analytics, Internet of Things (IoT), IT infrastructure, security, etc. IBM Cloud services include Infrastructure as a Service (IaaS), Software as a Service (SaaS) and Platform as a Service (PaaS).

The focus of this side paper is limited to the first three modules of the consultation, which are the most relevant with regards to IBM's experience and the services our company provides as a B2B cloud services provider.

For more than a century, IBM has earned the trust of our clients by responsibly managing their most valuable data, and we have worked to earn the trust of society by ushering powerful new technologies into the world responsibly and with clear purpose. IBM has for decades followed core principles – grounded in commitments to Trust and Transparency[1] – that guide its handling of client data and insights, and also its responsible development and deployment of new technologies, such as IBM Watson.

As a responsible company, IBM believes that the safety of users online is paramount and we encourage all technology companies to adopt similar principles to protect client data and insights, as well as prevent illegal content to spread across the Internet. This has become an even greater imperative at a time when the use of digital technologies has accelerated amidst the ongoing COVID-19 crisis and will be an essential part in the recovery of our society and economy.

[1] *https://www.ibm.com/blogs/policy/trust-principles/*

With greater digitization comes greater responsibility: digital services providers must ensure that technology remains a force for good and that the Digital Single Market in Europe remains a place where consumers are protected, have greater choice, and where businesses can compete fairly and thrive.

THE DIGITAL SERVICES ACT SHOULD SUPPORT EUROPE'S TRANSITION TO THE CLOUD

Cloud services providers, and particularly enterprise cloud, are a key source of competitive advantage and innovation for Europe. They have been particularly beneficial for SMEs and startups, and their uptake is accelerating in organizations of all sizes, driven by the cost reductions, flexibility, security and resilience that cloud-based services deliver. Enterprise cloud providers play a key role in helping Europe's objective to increase the digitization of industries and public services, as well as unlocking the potential of data faster and more securely.

Moreover, the COVID-19 crisis has made it even clearer that digitization is the central building block to ensuring the provision of essential public services, from healthcare to education, financial services or communications services. Business software and cloud computing services have also been essential in the sudden shift to remote working. Cloud technologies, but also AI, blockchain, IoT, data analytics etc. will continue to be crucial to increase the resilience of key sectors in Europe's economies.

IBM has been in Europe for over a century and is operating across the EU. We have a strong record on trust, responsibility and data stewardship and have invested in data centers across Europe that are state of the art in terms of security and privacy, designed to bring clients greater flexibility, transparency and control.

IBM has been supporting the digital transformation of the industry across all sectors: our clients include 10 of the largest global banks, nine of the top 10 retailers and eight of the top 10 airlines globally. Several large European companies have been using IBM Cloud services.

IBM has been a longstanding and active contributor to building technological capabilities in Europe, in line with its values. With the right approach, we believe the DSA can be an opportunity for Europe to champion online responsibility globally, and provide a safer, fairer and more innovative environment for the cloud.

EFFECTIVELY KEEPING USERS SAFER ONLINE

IBM believes that companies must be responsible for the societal effects of their online services, including facilitating criminal and terrorist activity and impacts on children and on elections. Therefore, **we fully support the DSA's objective** to establish new rules framing the responsibilities of digital services, addressing the risks and protecting the rights of users online.

We feel the European Commission should take a **"precision regulation"** approach, i.e. laws that include common-sense changes to the balance of regulatory and liability rules, yet are specifically tailored to consumer-focused platforms that not only host information but also make that information available to the public and have the technical means, practical ability, and the right to moderate content. Such an approach would hold such companies more accountable while avoiding one-size-fits-all, over-broad rules placing unnecessary burden on technology businesses, particularly SMEs and startups, and hinder innovation.

In the US, IBM recently played a key role in promoting passage of the SESTA/FOSTA[2] legislation to crackdown on the spread of online content, particularly against trafficking children for sexual exploitation. We continue to support reasonable, considered measures to regulate online activities that are clearly illegal globally.

1. MEASURES TAKEN BY IBM AGAINST THE ILLEGAL AND HARMFUL USE OF OUR SERVICES

Client data and the insights produced on IBM's Cloud or from IBM's AI are owned by IBM's clients. This is a core feature of our business model. As a provider of B2B cloud services, this is an essential difference between business models and services like ours, and consumer-oriented services such as social media platforms; video streaming services; or video, image, audio or file sharing services.

Because our clients' data belong to our clients, **we cannot remove specific content on our customers' websites, do not deploy any tools to monitor our clients' content and do not have the ability to identify illegal content ourselves**. Only our business customers have absolute control and responsibility over their own content and the services they operate.

[2] *https://www.ibm.com/blogs/policy/technology-responsibility/*

Our limitations to tackle illegal content are both technical and contractual:

- **Technical:** IBM does not have control over its clients' data. Additionally, clients may, and often do, choose to encrypt their data on our cloud infrastructure. We give our clients the ability to keep the encryption key and we do not have any access for security and privacy reasons.

- **Contractual:** our cloud services agreement limits the potential scope of IBM's access to, or use of, the client's content. In practice, this is a very limited right to access, and we do not have the right to monitor or modify the content.

As a responsible technology company, we do, however, have processes in place to tackle illegal usage of our services (as outlined in our Acceptable Use Policy[3]), which are as follows:

a. Notice & take-down

If we are made aware of the presence of illegal content on a client website, our abuse department will first assess the validity of the complaint from the content that is on the public website (NB: as IBM does not have any control over its business customers' data, it can only "see" what is visible on the public Internet and can only identify and inform the customer with whom IBM has a contractual relationship, who may be the party responsible for managing this content).

If the complaint is deemed valid, IBM will notify our customer asking the content to be removed expeditiously (or ask our customer to instruct their customer to remove it). If the customer fails to remove the content or to have it removed by the person/entity who uploaded it, according to the notified timeframe, IBM will suspend the service or block access to the server for that particular customer (NB: as IBM does not have the ability to remove the specific content directly, the only option is to shut down the server in its entirety).

Regarding the nature of the content itself, the vast majority of the complaints we receive involve content that is illegal because it infringes a trademark or copyright (IP). Most of the time (well over 90%) the actual publisher of the illegal content is not a direct customer of ours, but rather a customer of one of our customers.

[3] *https://www.ibm.com/services/us/imc/html/aup1.html*

b. Measures against other types of activities which might be harmful but are not, in themselves, illegal

IBM believes that **regulatory efforts should focus on illegal content and address harmful content separately**, such as through voluntary or co-regulatory approaches. In practice, IBM reserves the right to take measures against customers whose activities might not be illegal but may cause harm: our cloud services agreement[4] sets out various restrictions on how our services may be used, including "*unlawful, obscene, offensive or fraudulent content or activity, such as advocating or causing harm, interfering with or violating the integrity or security of a network or system, evading filters, sending unsolicited, abusive, or deceptive messages, viruses or harmful code, or violating third party rights*".

This broad language gives us the flexibility, in appropriate circumstances, to request our clients, if we believe they have violated the terms of our services agreement, to remove legal, yet harmful, content. We also reserve the right to suspend/terminate the services if the client fails to remove such content.

2. CLARIFYING RESPONSIBILITIES FOR ONLINE PLATFORMS AND OTHER DIGITAL SERVICES

IBM believes the **Commission's questionnaire could provide more clarity on how digital services should be differentiated**, particularly question 2.1 to identify what measures should be applicable to what types of platforms.

Differentiating the types of services and business models offered by platforms as opposed to their size or risk of exposure would be more appropriate to identify the platforms that are the best placed to act. Indeed, not all online platforms occupy the same space in the digital ecosystem: for example, an open source B2B cloud platform used to develop blockchain solutions for securing supply chains, and an aquaculture platform to keep salmon stocks healthy and make fish farming more sustainable, do not have the same societal impact when it comes to illegal content compared with video-sharing social networking service targeting young teenagers. Moreover, the B2B cloud provider developing the aquaculture platform is unlikely to have any control over the salmon farmer's data, as opposed to the video-sharing service that has a lot more technical ability to filter out illegal content before it's ever published.

[4] *https://www.ibm.com/support/customer/csol/contractexplorer/cloud/csa/be-en/10*

Additionally, certain platforms such as social media, link and share content for the purpose of generating advertising revenue, which is a very different business model than B2B services (generating revenues via on-demand/pay-as-you-go pricing; specific offering, etc.), thereby playing a very different role in the proliferation of illegal and harmful content.

A one-size-fits-all approach that would impose the same rules on all digital platforms would create disproportionate burden for many businesses that do not have the ability to control and moderate content, and do not disseminate content to the public such as B2B cloud services. Such an approach would limit the uptake of cloud technologies across businesses, particularly SMEs that may pose too great of a risk for any cloud provider to be prepared to take on should we be required, for example, to proactively monitor our customers' activities. This could lead to a chilling effect on innovation by SMEs in the EU and damage the broader data economy.

a. Defining the scope of the Digital Services Act

IBM believes that responsibility to tackle illegal content should rest with companies that are best placed to identify potential problems and take precautionary and remedial measures.

This is why we encourage the Commission to take a 'precision regulation' approach by ensuring that **additional obligations and liability specifically apply to online intermediaries that function as digital platforms for the purpose of exchanging, posting, and hosting publicly accessible content or information, and have the technical means, practical ability, and the right to moderate content.**

Specifically, we suggest that policymakers **define the scope of regulation to apply to**:

- Online services which disseminate content to the public such as public search engines, consumer application stores, B2C marketplaces and social media platforms.
- Online services whose main function is to allow peer-to-peer interactions, including the sharing and dissemination of content between consumers.

This means that we would recommend **excluding online intermediaries other than online platforms**, such as:

- Services which do not target consumers, or
- Other types of hosting services, which provide the backend infrastructure or that store content or data as part of a service provided to a company or another entity other than a natural person, such as webhosts, B2B services including enterprise cloud services, infrastructure services, DNS services, etc.

Imposing content monitoring requirements on cloud service providers would be onerous, disproportionate and is currently not possible for technical, contractual and business model reasons, as well as having serious implications for privacy and security. Only the enterprise customers have absolute control and responsibility over their own content and the services they operate. Therefore, our ability to respond to harmful content will generally be limited to suspending an entire service given our inability to edit individual items of content.

b. Know Your Customer (KYC) Policy:

IBM strongly supports rules that will protect consumers by preventing dishonest businesses selling illegal products online, but **such rules should avoid applying inappropriate constraints on B2B cloud services.** Setting stronger consumer protection rules should first take into account the role of digital services that are an active party in the provision of a B2C goods or services, while balancing the need to safeguard the smoothness and speed of online business operations. As an example, **digital services which are directed primarily at consumers, which act as the intermediary between the trader and the consumer or which provide the trading interface/platform for the online sale of consumer goods**, could be considered as relevant parties.

On the other hand, the provision of core services to regulated sectors such as operators of essential services depends entirely on the ability to provide robust cloud solutions that are neither designed nor intended to/directed at consumers. Moreover, enterprise cloud-based solutions are largely offered on a "Pay as You Go" principle, contributing to the success of the cloud.

IBM already implements strong safeguards to prevent fraudulent businesses from using our cloud services (e.g. contractual obligations in our service contracts, security-based services against fraud). Additional and disproportionate requirements may not only raise privacy and/or business confidentiality concerns, but could discourage companies, particularly SMEs and start-ups, from moving to the cloud, if held up from accessing services pending clearance.

Consequently, should regulators decide to include KYC measures in the future legislation, we would recommend a tailored approach, clarifying which consumer-facing services, sectors or activities require specific transparency criteria with the core objective of strengthening consumer protection standards.

CLARIFYING THE LIABILITY REGIME OF ONLINE INTERMEDIARIES

The e-Commerce has been an important framework to allow for the development of digital services, and we share the view that its main principles, such as the prohibition to impose a general monitoring obligation and the exemption of liability for online intermediaries, should be maintained. **However, IBM does not support the view that all online intermediaries should be exempt from liability by default**.

The e-Commerce Directive pre-dates the rise of social media services. Therefore, IBM believes that there is room to **further clarify under what conditions hosting services should be liable or not**.

More specifically, IBM believes that liability exemptions should be conditional on the appropriate hosting services applying a **standard of "reasonable care"** and taking actions and preventive measures to curb unlawful uses of their services. This standard should **specifically apply** to hosting services that are in a position to do something about illegal content, i.e. services that make that information available to the public and have the technical means, practical ability, and the right to moderate content.

This means, for example, ensuring that companies implement and enforce acceptable use policies and set up the necessary internal infrastructure (such as a 24/7 department for complaints tracking, clear processes for enforcement, etc.) in order to quickly identify and delete illegal content such as child pornography, violence on child-oriented sites, or online content promoting acts of mass violence, suicide, or the sale of illegal drugs.

This standard does not mean eliminating intermediary liability protections entirely, and many platforms have already implemented such measures. We simply believe online platforms should be held legally responsible to use reasonable, common-sense care when it comes to moderating online content.

Responsibility for exercising reasonable care should ultimately rest with those companies with the greatest practical ability to take action, not with every entity that may be connected to the value chain of building or managing the internet.

TACKLING ISSUES DERIVING FROM THE GATEKEEPER POWER OF DIGITAL PLATFORMS

IBM supports the Commission's initiative to explore possible ex ante rules so that large online platforms acting as Gatekeepers do not unfairly restrict the ability of businesses, including new entrants, to compete on the market.

IBM shares the Commission's concerns about how certain contractual terms or practices imposed by Gatekeeper platforms have resulted in consumer lock-in and deterred third parties from entering (or trying to enter) new markets. These platforms have adopted multiple strategies to protect their Gatekeeper role and to extend it. Indeed, the massive accumulation of data by Gatekeeper platforms allows them to entrench their position on their core or original markets and gives them an unparalleled advantage to enter neighboring markets, especially in comparison to third parties active on, or wanting to enter, these neighboring markets. Due to network effects, third parties are unable to create similar volumes of data which would allow them to operate profitably in the markets where the Gatekeeper platforms are active. This is particularly visible in areas such as Artificial Intelligence, where the quality of the product (including addressing potential bias) depends on the quality and amount of data used to train the product.

In this context, IBM would recommend the Commission to consider the following elements to correct potential imbalances and failures:

- **A clear and targeted definition** of "large online platforms acting as Gatekeeper" according to a **fixed set of cumulative criteria** focusing on the features that enable regulators to identify the platforms reaching such status (e.g. significant amount of consumer data, geographical coverage, user base), as opposed to anti-competitive behavior (e.g. customer lock-in, raising barriers to entry), which should be included in the list of prohibited practices (see below) but not as criteria to define Gatekeepers.

- **An "ex ante" regulatory tool geared towards a list of prohibited practices**, such as:
  - discriminating between competing products or services and their own services (self-preferencing);
  - hindering access to markets in which the platform is active, for example by imposing limitations on users/customers if they chose to procure products from third parties;

- using consumer data collected in one market to extend the platform's Gatekeeper role in another market and make it more difficult for third parties to access that market;
- transferring consumer data between B2C or B2B activities within the same group of entities, when these transfers result in client lock-in or barriers to entry;
- linking the sale of distinct services by which the Gatekeeper platform can promote new services/products through the sale of well-established products/services leading to customer lock-in and raise barriers to entry for third parties selling alternatives for the Gatekeeper platform's new services/products.

- **A dedicated regulatory authority** to impose behavioral remedies in order to effectively enforce such ex-ante tool.

The combination of the above elements would restore a level-playing field in the digital ecosystem, reduce market distortion and positively impact customer choice and innovation.

CONCLUSION

We welcome the Commission's decision to take a fresh look at the legal framework for digital services in Europe, and fully agree with the view that fostering innovation and competitiveness in the online environment will require clear, workable rules that can both ensure the safety of users while allowing digital businesses to grow and innovate.

Building trust in technology will first start with the need to acknowledge the legitimate concerns from governments, citizens and responsible companies around the behavior of some large online platforms, leading to the proliferation of illegal content online and causing market failures, such as limiting new entrants on the market or creating customer lock-in effects.

IBM believes that a **precision regulation approach** that is clear and targeted, i.e. identifying the specific business models and services that should be in scope, and defining tailored obligations scalable to the role and capabilities of such platforms, can help restore accountability and fairness in the digital ecosystem, while preserving the competitiveness of digital businesses.

We look forward to contributing to the debate in the months ahead.