RIPE NCC Position Paper on the Upcoming Digital Services Act

7/9/2020

Introduction

The European Commission's upcoming Digital Services Act will undoubtedly affect a wide range of online service providers in ways that will fundamentally affect their daily operations and, as a result, the ways in which the Internet is used and operates throughout the European Union and beyond.

Given the enormous impact of such legislation, the RIPE NCC is pleased to have an opportunity to express its opinions and concerns about the Digital Services Act, which we hope will be taken into consideration in updating the existing directive. Established in the Netherlands in 1992, the RIPE NCC has played an essential role in the Internet's development in Europe for nearly 30 years as one of the world's five Regional Internet Registries, responsible for the administration of Internet number resources (IP addresses and Autonomous System Numbers) throughout Europe, the Middle East and parts of Central Asia, and as the operator of K-root, one of the world's 13 root name servers that form the backbone of the Domain Name System (DNS).

With more than 20,000 members including Internet service providers, government agencies, banks, academic institutions, corporations and other large-scale network operators in 76 countries (including all EU member states), and as the secretariat for the RIPE community, which sets the policies governing Internet number resources in Europe and which has contributed feedback to this statement, we are also uniquely positioned to provide a neutral and expert high-level overview of how regulation could affect operators and infrastructure across different layers of the Internet.

The core is not the content

Although the Internet is often perceived as a single technology, it comprises many different components at many different layers that each have a role to play in its functioning. The Digital Services Act's focus on content regulation – specifically, in limiting illegal and potentially harmful content – is of course understandable given the myriad threats on the Internet today. However, we urge the European Commission to make a clear distinction between the Internet's core infrastructure and the source of those threats – namely, the applications and content that run on top of that infrastructure – and to protect the Internet's core infrastructure and operations from the potential for abuse as an unintended consequence of content regulation.

There needs to be a balance of responsibilities and liability

Without a clear understanding and protection of the Internet's public core in place, it will be far too easy to try to address illegal content by striking at the core infrastructure, including Internet routing and the Internet Protocol (IP) and DNS layers, rather than targeting the specific applications and content running on top of this infrastructure. While it can be easier to block IP addresses and domain names than it is to block specific content, the collateral damage that is likely to result from this "sledgehammer" approach has the potential to affect large segments of the Internet that had every right to continue functioning normally. Take down notices that lead to IP addresses (or even entire prefixes) and domain names being blocked can be very disruptive to the normal functioning of the Internet, and should be a last resort.

The possibility of extending the DSA to cover not only illegal but also "harmful" content also carries with it the potential for abuse. Together with a lack of adequate protection of the Internet's core infrastructure, and the possible inclusion of a "Good Samaritan" clause (which would protect providers who act in good faith to voluntarily and proactively take action against illegal material), this could end up resulting in a perfect storm, whereby the Digital Services Act would simply make it too easy to abuse the process to take action against online intermediaries.

For example, what would stop a bad actor from sending millions of automated notice-and-takedowns to a competitor as a kind of DDoS attack if there is no cost to her in requesting action against ambiguously defined "harmful" content, and yet the receiver is obligated to take action under very strict deadlines or face major penalties? Or from hiding behind the Good Samaritan clause and pretending to act in good faith in order to remove content for her own nefarious reasons? To keep this from happening, there must be a balance of liability between those removing content or requesting content be removed, and those receiving the requests for action.

A clear definition of what constitutes harmful content and dis/misinformation would be needed so that service providers have proper guidance in determining whether to respond to takedown notices, including clear guidelines on when different service providers can and should take action. A higher burden of proof should be required for any action that would affect the core infrastructure or operations, as well as some measure of shared liability or another deterrent against malicious motivations.

Arriving at clear definitions

In order to thwart this potential for abuse and ensure the effective application of any regulation that aims to deliver a legal framework for digital services, we must be able to separate core infrastructure and operations from applications and content – and yet, this is not an easy task.

While the current NIS Directive includes digital infrastructure as one of the sectors covered under "operators of essential services", it does not offer definitive guidelines on how to define these operators. When addressing the liability regime for intermediary service providers, there is a lot of ambiguity about how the three categories set out in Articles 12,13 and 14 of the E-Commerce Directive (mere conduit service providers, caching providers and

hosting providers) should be interpreted and whether, for example, operators providing DNS services and those involving routing/forwarding, including Internet exchange points, are meant to be covered by them – and yet these intermediaries play a vital role in the Internet's functioning and should be protected from political intervention.

A more helpful starting point may be found in the work of the Global Commission on the Stability of Cyberspace (GCSC)[1], which comprises members from different stakeholder groups across different regions, and which developed a Norm to Protect the Public Core of the Internet that advocates, "State and non-state actors should neither conduct nor knowingly allow activity that intentionally and substantially damages the general availability or integrity of the public core of the Internet, and therefore the stability of cyberspace." In its definition of the public core of the Internet, the GCSC includes a non-exhaustive list of core functions and elements, including packet routing and forwarding, naming and numbering systems, the cryptographic mechanisms of security and identity, transmission media, software, and data centres.

While arriving at a clear definition of the public core of the Internet and understanding how the different layers and operators affect one another is a complex task, we stress the importance of examining how the DSA could ultimately affect the Internet's general availability and operation. We must take a holistic approach by evaluating such impact from a functional rather than a purely technical perspective. The question should be: What will the effect be on the end users?

We must take a multistakeholder approach

In order to develop these needed definitions and understand how they will affect the many different types of online service providers, technical components and the functioning of all the different Internet layers, it is essential to invite members of the technical community, as well as all other affected stakeholders, to share their experiences and expertise. We applaud the European Commission in holding an open consultation through which different stakeholders can provide their feedback on the Digital Services Act, and would encourage the full participation of the technical community and all other stakeholders as much as possible throughout the legislative process.

Only through this multistakeholder approach – which has served the development of the open, innovative Internet so effectively since its conception – will the European Commission be able to table legislation that will continue to best serve the needs of Internet operators and users throughout the European Union.

Regulation should support innovation

The RIPE NCC believes that the ultimate goal of the DSA should be to protect the public core of the Internet from unnecessary intervention. Regulation should complement, not replace, the existing public-private partnerships that support the Internet's functioning. The European technical community responsible for key Internet functions already has processes

[1] https://cyberstability.org/

in place that have allowed it to lead the world in Internet development, and EU regulation should not hamper its ability to innovate. Only with the appropriate protections in place can the core infrastructure remain free to continue developing, ensuring that the Internet's potential to add value to our economies, societies and everyday lives can be fully realised.