ICLE tl;dr

Online Intermediaries and "Know Your Business Customer" Requirements

October 2020

tl;dr

Problem: It comes as no surprise to anyone that illegal conduct occurs online. Unfortunately, the individuals and businesses engaging in illegal activity may avoid detection by using tools that hide their identity. This makes enforcement difficult or even impossible.

Solution: In some cases, there may be targeted solutions available whereby intermediaries are required to record and verify the identity of business customers. In principle, this approach could be used to directly pursue parties actually liable for illicit content with minimal burden on either the platforms, or non-business customers.

KEY TAKEAWAYS

EU PROPOSES NEW KYBC REQUIREMENTS TO COMBAT ILLICIT MATERIAL ONLINE

In a recent policy paper, the EU recommended the introduction of "know your business customer" (KYBC) requirements for intermediary service providers in order to address the problem of "structurally infringing websites"—websites with a business model explicitly based on copyright infringement. The EU suggested that such KYBC requirements, which would essentially require the verification and recording of the identities of business customers, could be achieved using records maintained by the European Business Register or one the Ultimate Beneficial Owner Registers.

That would in principle enable the identification of websites owned by corporations based in the EU. The focus of the program would be on business customers, thus the report recommends limiting collection of data to commercial customers that will be "offering goods or services to consumers for purposes relating to their trade or business."

ICANN COULD ALSO ADOPT KYBC REQUIREMENTS

In some cases, firms may use technological barriers to hide their identities. One of the areas where this is particularly a problem is in accessing accurate beneficial ownership information of domain names.

ICANN is the organization that manages the worldwide domain name system (leaving aside China). Over the years, the WHOIS information that ICANN maintains on registered domains (such as contact information, organization name, and place of operation for a business) has become progressively less accurate.

One problem arose as organizations—known as "proxy registrants"—began to act as

third-party name registrants on behalf of customers who wished to remain anonymous.

There are good reasons to wish to remain private—for instance, publishing controversial material in a hostile regime. However, some proxy registrants not only protect the public distribution of private information, they also structure their businesses in a way to prevent anyone from ever being able to unmask a true operator of a domain name—even with valid legal process.

Currently, the WHOIS information that domain name providers collect ranges from accurate and capable of identifying parties when necessary to fully anonymized such that no legal process can ever be served on the owner of the domain. After GDPR was passed in the EU, the ability to access WHOIS information only became more difficult.

One possible solution to this problem would be the introduction of KYBC obligations on registrars as part of their contracts with ICANN.

KYBC SOLUTIONS ON THE HORIZON

Until recently, a global solution for requiring KYBC obligations on intermediaries was not generally practicable due to the absence of comprehensive business registries or beneficial ownership registries in many jurisdictions, including the U.S., and the relatively high costs of most verification of identity (VOI) systems.

Indeed, one of the reasons that such global systems are not popularly promoted is the risk that KYBC information stored on centralized servers might be stolen and used for nefarious purposes, as exemplified by the Equifax data breach.

However, with the development of secure digital identity registries by both the private and public sectors, the costs of VOI are likely to fall. According to the World Bank, 161 countries now have digital identity systems, although many are very basic.

In addition, new systems that use distributed ledger technologies to establish connections with trusted networks of VOI providers could dramatically reduce the risk of data breaches by storing information pseudonymously and sharing only limited information.

DUE PROCESS CONSTRAINTS

Even with the development of decentralized systems for storing VOI information, it would be important to constrain the disclosure of such information. So, any requirement for KYBC should be accompanied by a requirement that the such information only be disclosed pursuant to valid legal process.

CONTACT US

Julian Morris
Senior Scholar
jmorris@laweconcenter.org

Kristian Stout
Director of Innovation Policy
kstout@laweconcenter.org

ICLE International Center for Law & Economics