ICLE International Center for Law & Economics

Comments on the Advanced Notice Of Proposed Rulemaking, Re: Executive Order 13984, 'Taking Additional Steps To Address the National Emergency With Respect to Significant Malicious Cyber-Enabled Activities'
October 25, 2021
Kristian Stout

Intro and summary

As one of his final acts in office, former President Donald Trump signed Executive Order 13984 (the EO), "Taking Additional Steps To Address the National Emergency With Respect to Significant Malicious Cyber- Enabled Activities." The EO directed the Secretary of Commerce to "propose for notice and comment regulations that require United States IaaS providers to verify the identity of a foreign person that obtains an Account."

In its related advanced notice of proposed rulemaking (ANPRM), the U.S. Commerce Department notes that:

> …foreign persons obtain or offer for resale IaaS accounts (Accounts) with U.S. IaaS providers, and then use these Accounts to conduct malicious cyber-enabled activities against U.S. interests. Malicious actors then destroy evidence of their prior activities and transition to other services.
>
> This pattern makes it extremely difficult to track and obtain information on foreign malicious cyber actors and their activities in a timely manner, especially if U.S. IaaS providers do not maintain updated information and records of their customers or the lessees and sub-lessees of those customers.

The rule of law is frustrated when courts and law enforcement are unable to locate those who commit illegal acts. Other legal frictions may arise when the law fails to deter illegal behavior or to offer incentives for firms to adopt socially optimal business practices. These concerns are particularly acute online, because the Internet hosts a large volume of activity from anonymous or otherwise difficult-to-locate users.

The Internet's ability to facilitate anonymous or pseudonymous communications, of course, also continues a long tradition of anonymous speech being protected under U.S. constitutional law. The ANPRM acknowledged this tension when it asks "[c]an the Department implement the requirement to verify a foreign person's identity… while minimizing the impact on U.S. persons' opening or using such Accounts, or will the

application of the requirements to foreign persons in practice necessitate the application of that requirement across all customers?" But anonymity is just one value among many that must be weighed when crafting regulatory policy—particularly with respect to enforcing criminal law and upholding national security. Thus, even if the EO has some effect on U.S. business customers, that alone ought not foreclose implementation of effective identity-verification requirements.

Further, it is important to consider how the incentives service providers face align with optimal social policy. In particular, Information as a Service (IaaS) providers may not adequately internalize the social costs that stem from their making anonymous or pseudonymous accounts available to the public. Public policy may be necessary to correct such misalignment. While the EO focuses narrowly on the use of IaaS by foreign actors, there are broader problems associated with the anonymous use of Internet-connected services. As such, the Administration, the U.S. Commerce Department, and Congress should consider broader "know your business customer" (KYBC) requirements.

But while IaaS providers' potential misalignment of incentives is a proper subject for regulatory and legislative action, policy should be carefully calibrated to encourage compliance with broader criminal and national-security goals, while still permitting the vibrant IaaS industry to continue to thrive. The law must shape incentives such that responsibility to deal with illicit activity is placed where it is appropriate. Overly broad regulatory requirements can become burdensome, accrue more costs than benefits, and ultimately chill entry of new firms.

Thus, as described in more detail below, the EO is correct to require basic identity verification by IaaS providers, subject to some caveats. The goal of these regulations should be to collect the optimal amount of information about bad actors with the least interference in the operations of firms subject to the requirements. Thus, the Department must weigh how much benefit it realistically expects to obtain from any given level of compliance. Notably, the overwhelming number of IaaS accounts will be law-abiding users. The process is thus largely about identifying outliers, and regulatory intervention must be tempered in recognition that IaaS firms are constrained in the degree to which they can assist in furthering legitimate law-enforcement ends.

The requirements ought to be designed to obtain the optimal level of information that law enforcement and courts would need *in most, but not all, cases.* A minimal set of initial verification requirements, paired with an ongoing obligation to re-verify user identities, ought to resolve most problems associated with anonymous users.

Moreover, it would be highly inadvisable to prescribe specific technological measures that providers must use. Providers should be free to implement what they consider to be appropriate identity-verification systems, so long as those systems elicit the needed information. Relatedly, IaaS providers are bound by the requirements of laws like the EU's General Data Protection Regulation (GDPR) and therefore need the flexibility to design their systems to comply both with the Department's final rules as well as various privacy regimes

to which they are subject.

Read the full comments here.

View Article