Bureau of Industry and Security
U.S. Department of Commerce
1401 Constitution Ave NW
Washington, DC 20230

April 30, 2024

Re: Notice of Public Rulemaking on E.O. 13984, "Taking Additional Steps To Address the National Emergency With Respect to Significant Malicious Cyber-Enabled Activities," and E.O. 14110, "Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence." Docket No. DOC–2021–0007

Overbearing KYC Identity Requirements for Cloud Providers Put Consumers at Risk and Threaten Online Free Speech and Commerce

Dear Under Secretary Alan F. Estevez,

The Consumer Choice Center is an independent, non-partisan consumer advocacy group championing the benefits of freedom of choice, innovation, and abundance in everyday life.

As an organization representing consumers around the country, we are deeply concerned with the proposed rule to require significant Know Your Customer (KYC) procedures for any and all Infrastructure as a Service (IaaS) providers, as detailed in **Docket No. DOC-2021-0007**.

If these rules as they stand are brought into effect, they will have immediate consequences on consumers and online users who create, use, and deploy all manners of online services, servers, cloud systems, and virtual machines. This includes services that allow users to deploy servers to host their own private document and photo content, Bitcoin and cryptocurrency nodes, artificial intelligence models, Virtual Private Networks (VPNs), and more, in accordance with the terms of service offered by IaaS providers.

While these rules are intended to provide more immediate access to information and data on malicious foreign actors using American cloud infrastructure, they will instead result in significant risk to individual privacy, facilitate the loss or malicious use of data, and grant extraordinary powers to government agencies that are inconsistent with the US Constitution and the Bill of Rights.

We understand the intention is to target foreign hostile actors, but the requirement placed upon US service providers will inevitably require that every American provide this information as well.

The requirement that service providers maintain exhaustive personal and financial information on their customers presents not only a gross violation of privacy, but a significant risk, as the thousands of IaaS providers will be in possession of vast amounts of personal data liable to be hacked or leaked.

What's more, law enforcement agencies already possess enough tools and authority to follow legal processes to acquire warrants and conduct information.

We believe this proposed rule goes much too far in restricting the ability for Americans to use online services they want to choose, and would limit their ability to use servers and cloud services without significant risk to their privacy and personal data.

In addition, the exhaustive information required by a service that wishes to offer users the ability to run a virtual machine, server, AI model, or more, will necessarily push most Americans to opt out of using domestic services entirely, creating economic consequences not calculated in the proposed rule's costs of compliance.

We would recommend that this rule be revised entirely, removing the significant privacy risks that KYC collection on IaaS providers would require for domestic users, as well as the duplicative and extralegal authority that would be granted to law enforcement officers, in contravention of constitutional law.

Below, we list the two main areas of concern for US consumers.

KYC Requirements For Foreign Users Applied to Domestic Users

As noted in the Background provided in the Supplementary Information of the rule, these new powers would require service providers to segment users based upon their country of origin:

> To address these threats, the President issued E.O. 13984, "Taking Additional Steps To Address the National Emergency With Respect to Significant Malicious Cyber-Enabled Activities," which provides the Department with authority to require U.S. IaaS providers to verify the identity of foreign users of U.S. IaaS products, to issue standards and procedures that the Department may use to make a finding to exempt IaaS providers from such a requirement, to impose recordkeeping obligations with respect to foreign users of U.S. IaaS products, and to limit certain foreign actors' access to U.S. IaaS products in appropriate circumstances.

However, in order for IaaS providers to effectively determine the location of a user, they will be required by the force of law – and risk of civil and criminal penalties – to log, categorize, and document a user's location and accompanying personal information regardless of their location, all in efforts of determining whether a potential user would be considered a "foreign user" or beneficial person.

This will lead to increased collection of information akin to bank accounts and financial transactions, leading to widespread "Know Your Customer" (KYC) requirements which have never been applied at this level to online services.

Beyond congressional approval, we believe this proposed regulation far exceeds the bounds of agency authority, whether from the Department of Commerce or via the mentioned Executive Orders, and would create significant areas of risk for ordinary users and customers location both abroad and within the United States.

In addition, the broad application and definition of a covered service – "any product or service offered to a consumer, including complimentary or "trial" offerings, that provides processing, storage, networks, or other fundamental computing resources, and with which the consumer is able to deploy and run software that is not predefined, including operating systems and applications" – essentially means any cloud service would be within the scope of this regulation.

The Risk of Privacy Breaches

As service providers would be required to maintain a robust Customer Identification Program, as outlined in § 7.302, this would therefore place liability on all cloud providers to collect and retain the full name, address, credit card number, virtual currency numbers, email, telephone numbers, IP addresses, and more on any potential customer of their service.

While we appreciate that private cloud providers and IaaS firms would have the latitude to determine how they structure their Customer Identification Programs, we believe that the requirement to collect this information and store it locally will constitute a high potential for that information to be accessed without authorization, either by hacks, leaks, or other malicious activity.

Because service providers will be required to catalog this information for years on end, this will inevitably prove to be a high-value target for malicious actors, while providing minimal benefit to the law enforcement agencies that can already legally obtain this information via lawfully executed warrants.

Extraordinary and Duplicative Powers

Law enforcement agencies at the federal, state, and local level already possess the legal tools to subpoena or request data cloud providers or VPN providers with lawfully obtained warrants.

That IaaS providers would be required to not only retain this information, but also to preemptively "notify" law enforcement without any judicial order or suspicion of a crime, violates the Fourth Amendment and the Due Process Clause as interpreted from the Fifth and Fourteenth Amendments.

Section § 7.306(d) lays out the stipulation for being exempted from the requirements as "voluntary cooperation" with law enforcement agencies, then forcing providers to enable access to "forensic information for investigations of identified malicious cyber-enabled activities".

We believe this would be easily abused, as it would provide a legal path for companies to divulge customer information to government authorities beyond what is necessary and lawful, and provide incentives for firms and companies to voluntarily submit information on their customers to government agencies, law enforcement agents, and more.

As written, we believe this proposed rule has been offered in haste, and will likely lead to significant harms and risks to consumers' data, privacy, and their liberty to engage in free commerce. We would urge this rule to be rewritten with these concerns in mind.

Sincerely yours,

Yaël Ossowski
Deputy Director,
Consumer Choice Center