October 25, 2021

Trisha B. Anderson
Deputy Assistant Secretary Intelligence & Security
U.S. Department of Commerce
1401 Constitution Ave. NW
Washington, DC 20230

Re: Comments Responding to Advance Notice of Proposed Rulemaking (ANPRM) Regarding The development of Regulations pursuant to Executive Order 13984

Dear Ms. Anderson:

These comments are submitted in response to the ANPRM on "Taking Additional Steps to Address the National Emergency with Respect to Significant Malicious Cyber-Enabled Activities."

I am a scholar and teacher of intellectual property and information security law at the University of Akron School of Law, where I am the Goodyear Endowed Chair in Intellectual Property Law. I am also a Senior Fellow at the Geneva Network, a think tank that focuses on global trade and innovation policy. In the latter capacity, I have filed comments with the European Commission on its proposed Know Your Business Customer regulations. My comments reflect my own views based on my prior academic and policy research.

The Need for Know Your Business Customer Regulations

While motivated by valid concerns regarding foreign actors use of Infrastructure as a Service (IaaS) accounts to conduct malicious cyber activities, E.O. 13984 is founded on a core principle that online service providers should do due diligence regarding the identity of their customers. In other contexts, this principle of due diligence regarding customers has been framed as Know Your Business Customer, or KYBC. My comments address why KYBC could lead to a long overdue and much needed rebalancing of online rights and obligations.

In the late 1990s, the U.S. created a regulatory framework for online business that largely relieved them of responsibilities that brick and mortar businesses have when dealing with customers. Businesses are largely shielded from liability for enabling or facilitating their customers' online wrongdoing by the Section 230 of the CDA as well as the safe harbors of the Digital Millennium Copyright Act.

This approach purposefully cleared a path for online businesses with the hope that they would develop their full potential. By largely by relieving them of responsibilities required of offline competitors, the hope was that they would grow quickly from their infancy

This approach yielded robust results, although perhaps not exactly the results originally intended or anticipated. On the one hand, innovation flourished, and the world now enjoys a vast digital marketplace. On the other hand, the rules shaped the types of businesses that flourished online,

opening a path for businesses that followed the opportunities created by liability shields and limited responsibilities.

While internet technology facilitates anonymity in communications, anonymity as an online business norm is a product of the regulatory environment. The nature of the regulatory framework creates incentives to demand little of one's customers and to "look the other way." While not all service providers are indifferent to their customers' behavior, the regulatory framework (or lack thereof) creates an opportunity for those who are.

This is contrary to how the law has traditionally worked, as it tends to incentivize traditional, offline businesses to know with whom they are dealing. The potential for indirect liability for one's customers actions makes businesses vigilant.

While these IaaS providers and other online plaforms provide desirable services, they often avoid the obligations that an offline business would have to protect consumer. The anonymity they foster makes it hard for other businesses and consumers suffering fraud or other injury to obtain recourse. It is difficult to help other businesses and consumers find and hold accountable those who use their platforms to communicate or sell goods. And, as the E.O. recognizes, this anonymity and lack of accountability can pose a significant cybersecurity risk.

The current regulatory framework was designed in the 1990s to shield and foster infant industries. The infant businesses of the turn of the century are now among the world's wealthiest, most powerful, and technologically adept businesses. They no longer need special protection, and society no longer benefits from it.

The E.O. presents an opportunity to move toward greater transparency and accountability online, correcting the unintended consequences of exempting online businesses from the responsibilities and accountability imposed on other businesses.

The E.O. also represents an opportunity for the U.S. to provide leadership in creating a safer online environment. The European Union is currently considering a Know Your Business Customer obligation as part of its proposed reform of the E.U.'s Digital Services Act. These developments in the E.U. are welcome, but it is important for the U.S. to lead rather than follow on this important issue.

Responses to Questions Posed in the ANPRM

I write primarily to respond to the following questions posed in the ANPRM:

> 1(a). How should the Department implement the requirement for both verifying a foreign person's identity (1) upon the opening of an Account, and (2) during the ''maintenance of an existing Account,'' and what should the Department consider in determining customer due diligence requirements for U.S. IaaS providers?

Strengthening the responsibility of IaaS providers and encouraging greater transparency is a key component of reforming and modernising the regulatory framework for online business. I suggest that the following principles will help achieve this responsibility:

- **A Level Playing Field.** Online and offline businesses should be subject to the same obligations and legal liabilities. Online regulation should follow the fundamental principle that "what is illegal offline is also illegal online."

- **A Fair and Safe Online Environment.** Online business models should not be founded on opportunities created by liability shields and regulatory gaps. Rather, online businesses should be required to deal fairly with and respect the rights of consumers and other businesses, just as they would offline.

- **A Free and Efficient Marketplace.** Regulation should preserve the free movement of digital services and a free marketplace. It should take the particular circumstances of online businesses. Preserving a free and efficient market does not require excusing online platforms from responsibility, however, but rather the same common sense regulation to which offline businesses are subjected.

In keeping with these principles, IaaS providers should verify and retain information regarding the businesses with which they are dealing – to Know their Business Customers (KYBC). Simply put, KYBC principles should require IaaS providers to verify the identity of customers so that other businesses and consumers could find and get a remedy from platform users who harm them. This requirement would create a more level playing field between online and offline businesses while fostering a safer and fairer online environment.

KYBC would level the playing field between online and offline businesses by imposing on them practices widely followed in the business world as either (or both) a matter of best practice and regulation. In many contexts, offline businesses find it in their best interest to know who their customers are, perhaps more so than online businesses, because physical resources can be wasted, lost, or damaged where digital ones are less vulnerable and scarce. Thus, a commercial landlord will need to know who its tenants are and how to reach them, whereas an online business may not be as concerned.

Even where offline businesses might find it useful, or profitable, not to ask too many questions of their business customers, the law often intervenes to protect consumers and society. Thus, a physical market owner may find itself liable if it tolerates or harbors fraudulent sellers. Also, and in particular, the financial industry has increasingly been regulated with the imposition of Know Your Customer (KYC) requirements. KYC requirements have become a familiar and important part of the regulatory landscape, imposed to combat money laundering and increase transparency in the wake of the Global Financial Crisis in 2007.

Past experience in the financial industry can guide implementation of KYBC requirements with respect to IaaS providers.

A KYBC requirement can and should also meet the principle of making the digital marketplace more efficient and free. Information requirements should be standardized, and, at least initially, rely on pre-existing sources of identification. In the long run, it would be useful to develop standards for portable, global, and user-owned digital credentials, using blockchain or other technology. A KYBC requirement need not be onerous in its implementation, and with proper care, requirements can increase efficiency and transparency in the marketplace.

> 1(b). Can the Department implement the requirement to verify a foreign person's identity (1) upon the opening of an Account, and (2) during the ''maintenance of an existing Account,'' 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?

A KYBC requirement will likely need to be applied to all customers to be effective. The need to verify whether a business is a U.S. person is already a significant step toward KYBC. Moreover, exempting U.S. businesses from the requirement would just encourage the worst actors to evade the requirement by masquerading as U.S. entities.

In conclusion, E.O. 13984 presents an opportunity to implement a KYBC requirement for IaaS provider, which would be a modest, but significant reform toward bringing U.S. e-commerce regulation into the 21st Century. If done properly, it can meet key goals of leveling the playing field between online and offline businesses, ensuring a fair and safe online marketplace, and making e-commerce more transparent and efficient.

Thank you for the opportunity to comment.

Sincerely,

Mark Schultz
Goodyear Tire & Rubber Company Endowed Chair in Intellectual Property Law
Director, Intellectual Property & Technology Law Center
The University of Akron School of Law