Before the
U.S. Department of Commerce
Washington, D.C. 20230

In re:	)	
	)	
Taking Additional Steps to Address	)	DOC-2021-0007
the National Emergency With Respect	)	RIN 0605-AA61
to Significant Malicious Cyber-Enabled	)	
Activities	)	

Comments of Online Safety Organizations in Response to the Advanced Notice of Proposed Rulemaking

Oct. 25, 2021

Table of Contents

I. Overview

Internet intermediaries' failure to verify their customers' identities aggravates today's growing epidemic of harmful and illegal conduct online in two ways. First, people are more likely to engage in antisocial and unlawful conduct if they believe their identities are hidden. Second, holding individuals and entities accountable becomes harder if no one knows who they are.

As online safety organizations, we recognize the value of anonymity. People often have good reasons for protecting their identities, such as securing their safety from those who would cause them harm and avoiding retribution for whistleblowing. Verifying identities for use of internet services can occur, however, while maintaining safeguards that prevent disclosure except in appropriate circumstances. The guiding principle should be protecting the privacy and safety of law-abiding individuals and the public, not protecting the privacy of criminals engaging in the invasion of others' privacy—or worse.

The undersigned groups therefore welcome this advanced notice of proposed rulemaking to implement Executive Order 13989, which directs the Department of Commerce to adopt regulations requiring that internet "infrastructure as a service" providers verify the identities of foreign individuals and entities seeking to use the IaaS providers' services.[1] Federal efforts to ensure users of internet services provide their true identities—at least to the internet intermediaries they use, if not publicly—would go a long way toward preventing bad actors from engaging in, or evading accountability for, harmful and unlawful conduct. Consequently, we make the following recommendations:

- The Department should implement and apply the executive order's verification requirement as broadly as possible, both in terms of what types of providers must abide by the requirement and what customers the providers must verify.

[1] *See In re*: Taking Additional Steps to Address the National Emergency With Respect to Significant Malicious Cyber-Enabled Activities, DOC-2021-0007, *Advanced Notice of Proposed Rulemaking*, 86 Fed. Reg. 53018 (Sept. 24, 2021); Exec. Order No. 13984, 86 Fed. Reg. 6837 (Jan. 25, 2021).

- The Department should model the verification requirement after the financial industry's Know Your Customer requirements.

- To further reduce the already minimal risk of conflicts with international, federal, and state laws—and to provide additional policy benefits—the U.S. government should enact the Shop Safe Act, the Inform Consumers Act, WHOIS legislation, and other KYC-type laws, and include identity verification requirements in trade agreements.

- The Department should not wait until after malicious cyberattacks cause harm to enforce the verification requirement against recalcitrant providers but should conduct periodic audits to reduce the number of attacks in the first place.

- The Department should not grant exemptions to, or allow self-certification of, the verification requirement, although adoption of security best practices approved by the Commerce Department could be evidence of compliance.

II. The Need for Internet Intermediaries to Act Responsibly

The internet is a revolutionary tool. But like any tool, it can be abused. Bad actors increasingly use the internet to engage in harmful and unlawful activity, such as fraud, identity theft and theft of personal information, spread of malware, sale of counterfeit and unsafe products, looting of antiquities, wildlife trafficking, trafficking of human remains, civil rights violations, harassment, illegal drug sales, nonconsensual dissemination of intimate images, distribution of child sexual abuse materials, cyberattacks, espionage, and terrorism.

One of the great strengths of the internet is its distributed nature. No single, centralized entity controls what happens online. That enables people and organizations across the globe to contribute to the internet's architecture and content. Yet precisely because myriad intermediaries facilitate any and all activities on the internet, no single individual or entity can solve problems that arise. Responsible, proactive action by online intermediaries—such as search engines, domain name providers, web hosting operators, reverse proxy services, online payment processors, internet advertising networks, online marketplaces, and social media platforms—can go a long way toward ensuring the internet is a safe place for people, especially children, to interact.

Much of that responsible, proactive activity can happen through voluntary initiatives. Most online intermediaries reserve the right in their terms of service to stop harmful and unlawful conduct and to terminate the accounts of users who engage in such behavior. Consistently enforcing these policies would make a big difference. As part of doing so, internet intermediaries can collaborate with private sector and public interest organizations to craft effective tools and practices for addressing illegal activity. Some of that occurs today. We hope such efforts will grow, and that the U.S. government will continue to support and incentivize them.

But if voluntary solutions were sufficient to protect people, societies never would have needed to enact laws. Many of the scandals occupying news headlines and congressional hearing rooms today stem from internet intermediaries' failure to adequately moderate harmful and unlawful activity and consistently apply their terms of service. That is why Congress is considering reforming section 230 of the Communications Act, which as currently interpreted by the courts grants internet intermediaries immunity even when they negligently, recklessly, or knowingly facilitate unlawful and harmful conduct by their users.[2]

III. The Importance of Verifying Identities Online

Verifying identities is one important element of promoting a safe and secure internet. Recognizing this, the House Judiciary Committee recently passed the bipartisan Shop Safe Act by a 30-8 vote.[3] The Shop Safe Act would subject an online marketplace to potential civil liability for contributory trademark infringement if it failed to verify the identity of a seller on its service and that seller sold counterfeit goods implicating health and safety. The Senate has a companion bill.[4]

[2] *See* Neil Fried, *Why Section 230 Isn't Really a Good Samaritan Provision* (Mar. 24, 2021), https://digitalfrontiersadvocacy.com/blogs-and-op-eds/f/why-section-230-isnt-really-a-good-samaritan-provision.

[3] H.R. 3429, 117th Cong., (as reported by the H. Comm. on the Judiciary, Sept. 29, 2021).

[4] S. 1843, 117th Cong. (referred to the S. Comm. on the Judiciary, May 26, 2021).

The Senate has also introduced the bipartisan Inform Consumers Act, which would require online marketplaces to verify the identity of "high-volume" sellers.[5] Just as the Senate has a companion bill to the Shop Safe Act, the House has a companion bill to the Inform Consumers Act.[6]

The availability of WHOIS data—which contains basic contact details for holders of internet domain names—is also critically important. WHOIS data has been public since the founding of the commercial internet and forms the basis of online transparency, security, and accountability. Access to that information is necessary to protect consumer privacy, promote lawful commerce, and ensure public safety. Indeed, a DOJ cyber report states that "[t]he first step in online reconnaissance often involves use of the Internet Corporation for Assigned Names and Numbers' WHOIS database."[7] A 2018 investigation by FireEye using domain name registration data, for example, discovered more than 2,800 inauthentic social media accounts originating from Iran that were designed to impersonate U.S. political candidates and influence media campaigns involving Iranian interests.[8]

Domain name providers often fail to verify WHOIS information, however, and in 2018 providers increasingly began restricting access to the data based on an overapplication of the European Union's General Data Protection Regulation. This is hindering efforts by cybersecurity firms, public interest groups, the private sector, federal agencies, and law enforcement authorities

[5] S. 936, 117th Cong. (introduced Mar. 23, 2021).

[6] *See Schakowsky Introduces Bill to Protect Consumers Making Purchases Online*, Press Release (Oct. 5, 2021) (stating that Reps. Jan Schakowsky (D-Ill.) and Gus Bilirakis (R-Fla.) have introduced the Inform Consumers Act), https://schakowsky.house.gov/media/press-releases/schakowsky-introduces-bill-protect-consumers-making-online-purchases.

[7] DOJ, REPORT OF THE ATTORNEY GENERAL'S CYBER DIGITAL TASK FORCE 35 (July 2018), https://www.justice.gov/ag/page/file/1076696/download.

[8] *See* FIREEYE, SUSPECTED IRANIAN INFLUENCE OPERATION LEVERAGING INAUTHENTIC NEWS SITES AND SOCIAL MEDIA AIMED AT U.S., U.K., AND OTHER AUDIENCES (2018), https://www.mandiant.com/resources/report-suspected-iranian-influence-operation.

to thwart online lawlessness—including identity theft, fraud, illegal sale of opioids, human trafficking, state-sponsored espionage, and terrorism.[9]

A 2018 survey of 55 global law enforcement agencies, for example, revealed that 98 percent found the WHOIS system aided their investigative needs before domain name providers took these unnecessary restrictive measures, as compared to 33 percent after.[10] More recently, a 2021 survey by two cybersecurity working groups found that restricted access to WHOIS data is impeding investigations of cyberattacks.[11] Two-thirds of the 277 respondents said that their ability to detect malicious domains has decreased, 70 percent indicated that they can no longer address threats in a timely manner, and more than 80 percent reported that the time it takes to address abuse has increased, which means that cyberattacks—and harm to victims—last longer.[12]

The U.S. Department of Homeland Security has similarly identified the lack of access to WHOIS data as a significant and growing problem. The DHS stated in a July 16, 2020, letter to Rep. Bob Latta, then chairman of the House Commerce Committee's Consumer Protection Subcommittee, that if the agency "had increased and timely access to registrant data, the agency would have a quicker response to criminal activity incidents and have better success in the

[9]*See, e.g.*, Natalia Drozdiak, *EU Privacy Laws May Be Hampering Pursuit of Terrorists*, BLOOMBERG, July 7, 2019 (reporting that U.S., European, and Canadian law enforcement used WHOIS data to identify approximately 400 domains registered to terrorist group Islamic State and make arrests; quoting Europol official Gregory Mounier's observation that "[s]ince May 2018, [Europol has had] more and more cases of investigations that are just dropped or severely delayed because we can't have direct access to WHOIS registration data information"), https://www.bloomberg.com/news/articles/2019-07-08/european-privacy-laws-may-be-hampering-those-catching-terrorists.

[10]Laureen Kapin, FTC Counsel for International Consumer Protection & Co-Chair, ICANN Public Safety Working Group, ICANN63 GAC Plenary Meeting 8 (Oct. 23, 2018), https://gac.icann.org/presentations/icann63%20pswg.pdf.

[11]*See* MESSAGING, MALWARE AND MOBILE ANTI-ABUSE WORKING GROUP AND THE ANTI-PHISHING WORKING GROUP, ICANN, GDPR, AND THE WHOIS: A USERS SURVEY—THREE YEARS LATER (June 2021), https://www.m3aawg.org/sites/default/files/m3aawg_apwg_whois_user_survey_report_2021.pdf.

[12]*Id.* at 6, 7, 20.

investigative process before criminals move their activity to a different domain."[13] The FTC and FDA have also expressed concern.[14]

The Department of Commerce has been outspoken about the United States' concern over the removal of public access to accurate WHOIS information.[15] The Department sent a letter as far back as April 4, 2019, directing ICANN "to deliberately and *swiftly* create a system that allows for third parties with legitimate interests, like law enforcement, IP rights holders, and cybersecurity researchers to access non-public data critical to fulfilling their missions."[16] The letter observed that "[w]ithout clear and meaningful progress, alternative solutions such as calls for domestic legislation will only intensify and be considered."[17] Senator Roger Wicker, then chairman of the Commerce Committee, echoed that sentiment in a May 6, 2019, letter to the Department of Commerce, stating that "[a]bsent a meaningful resolution to these issues, Federal legislation guaranteeing access to WHOIS data may be warranted."[18]

Yet, to this day, ICANN has failed to solve the problem. Noting the lack of progress, the Commerce Department sent Sen. Wicker a letter Dec. 23, 2020, "encourag[ing] the Committee to explore alternate approaches to providing federal and local law enforcement, cybersecurity

[13]Letter from Raymond Kovacic, Assistant Director, Office of Congressional Relations, DHS, to Rep. Bob Latta (July 16, 2020).

[14]*See* Letter from Joseph Simons, FTC Chairman, to Rep. Bob Latta (July 30, 2020) (expressing concern over new domain name provider policies "that significantly limit the publicly available contact information relating to domain name registrants" and stating that "[t]he FTC would benefit from greater and swifter access to domain name registration data."); Letter from Karas Gross, Associate Commissioner for Legislative Affairs, FDA, to Rep. Bob Latta (Aug. 13, 2020) (stating that "[a]ccess to WHOIS information has been a critical aspect of FDA's mission to protect public health" and that the reduced availability of WHOIS data "has had a detrimental impact on FDA's ability to pursue advisory and enforcement actions as well as civil and criminal relief in our efforts to protect consumers and patients.").

[15]*See*, *e.g.*, Remarks of David J. Redl, Assistant Secretary of Commerce for Communications and Information, ICANN 61 (Mar. 12, 2018), https://www.ntia.doc.gov/speechtestimony/2018/remarks-assistant-secretary-redl-icann-61.

[16]Letter from David J. Redl, Assistant Secretary of Commerce for Communications and Information, to Cherine Chalaby, Chair, ICANN Board of Directors (April 4, 2019).

[17]*Id.*

[18]Letter from Sen. Roger Wicker, Chairman, U.S. Senate Committee on Commerce, Science, and Transportation, to David Redl, Assistant Secretary for Communications and Information, U.S. Department of Commerce (May 6, 2019).

industries, the business and the IP communities—as well as small businesses and the public—prompt and effective access to information they need to build a safe, secure, and trustworthy internet."[19]

In light of the ongoing difficulties, we ask the Department of Commerce to advocate for a legislative solution. The Administration should also seek robust WHOIS access requirements in future trade agreements, perhaps expanding on language included in the U.S.-Mexico-Canada Agreement to apply to more than just a nation's country-code top-level domain.[20]

The same concerns that demand KYC-type regulations requiring providers of internet infrastructure to verify the identities of their customers also demand enactment of the Shop Safe Act, the Inform Consumers Act, WHOIS disclosure requirements, trade agreements that include identification verification provisions, and section 230 reform.

IV. Responses to Specific Questions

Below we provide answers to some of the Department's specific questions.

Question (1)(a): The Department asks how it should implement the requirement in Executive Order 13989 that U.S. IaaS providers verify a foreign customer's identity and contact information, both when the customer opens an account and periodically thereafter to ensure the information remains accurate. The process could be as simple as asking prospective customers to provide the information specified in the executive order: name, national identification number, address, source of payment (such as bank account, debit card, or credit card information), email

[19]Letter from Carolyn Tatum Roddy, Acting Assistant Secretary for Communications and Information, Dep't of Commerce, to Sen. Wicker (Dec. 23, 2020).

[20]United States-Mexico-Canada Agreement, art. 20.C.11(1)(b) (requiring each nation, in connection with the management of its country-code top-level domain, to provide online public access to a database of domain name registrant contact information, subject to each nation's law and, if applicable, relevant privacy and data protection policies), https://ustr.gov/sites/default/files/files/agreements/FTA/USMCA/20%20Intellectual%20Property.pdf.

address, phone number, and internet protocol address,[21] as well as perhaps a copy of government-issued photographic identification. The provider would also collect contact information for a representative where the customer will receive service, if different from the customer.

The provider should request payment information even if it does not charge for service. Doing so would provide additional data to check for accuracy and also leverage the due diligence that financial institutions will already have done pursuant to their own KYC requirements. The provider should also send the customer a physical confirmation notice to help ensure that the service request came from an authorized representative and not an imposter.

The provider would then cross-check the information against existing data sources. If the information appears inaccurate in a significant way, the service provider would refuse to provide service until the customer corrected the information. The provider would also inform the customer that a failure to keep the information up to date will result in termination of service. The provider would then periodically re-check the information.

Question (1)(b): The Department asks whether it can require providers to verify identification information only for prospective customers that are foreign or if verifying information for foreign customers will in practice also result in verification of U.S-based customers' identities. We think the latter.

To limit the verification process to prospective customers that are foreign, the provider would need reliable information about the prospective customers' identities, creating a Catch 22. Because the verification process will not be cumbersome for providers or (legitimate) customers, verifying the identities of all prospective customers—not just those that are foreign—will not be problematic, even with the obligation to keep the information up to date. Ironically, limiting the

[21] *See* Exec. Order No. 13984, § 1(a)(ii), 86 Fed. Reg. 6837, 6838 (Jan. 25, 2021).

requirement to prospective foreign customers, if even possible, might end up being more cumbersome for providers. Because U.S. customers are no less capable of using internet services to cause harm, the incidental verification of U.S. customers will also have value.

Question (1)(h): The Department asks how it might minimize the burden on providers to verify and maintain the identification information. Because collecting and cross-checking basic contact and financial information for prospective customers is not burdensome, no minimization is necessary.

Question (2): The Department asks about the data protection and security implications of requiring verification and retention of foreign customer identification information, including how the EU's GDPR, California law, or other state laws might apply. IaaS providers should, of course, safeguard the information they collect about foreign and domestic customers as required by applicable international and U.S. laws. International and domestic privacy laws generally allow, however, the collection, maintenance, and disclosure of identifying information for purposes of public safety, law enforcement, or compliance with national laws, as well as to enable a service provider to render service and send a bill to (the right) customers. Consequently, neither domestic nor international laws should hinder the Department's implementation of the executive order or the providers' compliance with the Department's rules implementing that order.

Question (3): The Department asks what other international implications for U.S. providers it should be aware of when designing the verification rules, and how it might mitigate the risk of negative international consequences. As discussed above, privacy laws typically allow collection and disclosure of personally identifiable information for legitimate purposes, such as public safety, law enforcement, and compliance with national laws, which will minimize the likelihood of any international issues.

There are steps the U.S. government could take, however, that would themselves have positive policy benefits while further reducing what little risk there may be of conflict with international and domestic laws. They include enacting the Shop Safe Act, the Inform Consumers Act, and WHOIS legislation, along with other KYC-type laws, as discussed above. Enactment of such requirements would help make clear that when providers verify customer identities, they are doing so for public safety reasons and to comply with U.S. federal law, and thus that their collection, maintenance, and potential disclosure of that data falls within exceptions in international law. We therefore encourage the Department to support enactment of such laws and the inclusion of online verification provisions in trade agreements going forward.

Question (4): The Department asks how it should enforce the verification requirements. Because malicious use of internet infrastructure can cause serious harm, and because verification requirements are meant to prevent such harms, the Department should not check compliance and enforce the verification rules only after a malicious attack. Rather, it should minimize the odds of a malicious attack in the first place by conducting periodic audits.

Question (5)(a): The Department asks whether it should provide blanket exemptions from the verification requirements for providers that comply with security best practices, or whether it should grant only time-limited exemptions. Although the Executive order allows the Department to grant exemptions, we do not believe it should do so.

Providers that follow security best practices may find they are already in compliance with the verification rules that the Department adopts, and that the providers therefore do not need to implement additional processes. Certified compliance with security best practices promulgated by certain, recognized organizations might also be good evidence of compliance with the Department's verification rules.

Compliance with security best practices should not be a substitute for compliance with the verification rules, however. As discussed above, compliance with the verification rules will not be cumbersome. Moreover, even providers that comply with security best practices may have customers that engage in unlawful activity. Having verified identification information in such circumstances will be important.

If the Department nonetheless grants exemptions, those exemptions should be time-limited. Upon expiration of the time limitation, the Department should require providers to demonstrate that they are still in compliance with security best practices, especially since such best practices and the threats they are designed to combat will change over time. The Department should also require organizations that promulgate security best practices the Department relies on to periodically submit those practices for Department review. In addition, only organizations and practices that the Department has sought comment on, reviewed, and approved should be used for purposes of the exemptions.

Question (5)(c): The Department asks what industry standards or best practices it should use to assess the appropriateness of exemptions. As discussed above, we do not believe the Department should create exemptions but, if it does, those exemptions should only be based on standards and best practices it seeks comments on and approves.

Question (5)(d): The Department asks how a framework for best practices might account for ever-evolving threats. That dynamic threat environment is precisely why, as discussed above, we believe the Department should not create exemptions to the verification requirements but should instead conduct periodic audits. It is also why, if the Department nonetheless creates an exemption process, those exemptions should be time-limited and based only on best practices that the Department approves and periodically reviews.

Question (5)(e): The Department asks how it should assess compliance with any security best practices for purposes of determining whether to grant exemptions, and if it should allow providers to self-certify. As discussed above, we do not believe the Department should create exemptions to the verification requirements. If it nonetheless does, it should not allow self-certification. The harm from malicious use of internet infrastructure can be serious, warranting periodic audits of compliance with the best practices by either the Department or third parties the Department approves.

Question (12): The Department seeks comment on how it should define certain terms. The Department should define relevant terms as broadly as possible. As discussed above, the failure of internet intermediaries to verify the identity of customers is a significant problem with far-reaching and serious consequences. The more broadly the Department applies its requirements for IaaS providers to verify the identities of their customers, the safer the public will be.

Question (13): The Department asks what differences in industry makeup, market dynamics, and general business practices it should take into consideration when implementing the verification requirements. Because of the flexible, interconnected nature of the cloud and IaaS products, malicious actors can use them to cause serious and widespread harm. Thus, the specific characteristics of a (potentially fraudulent) customer's use, or the particular characteristics of the IaaS provider's products and line of business, may not be directly related to the consequences that can result from misuse of the IaaS products. We therefore recommend that the Department not try to tailor its rules to the nature of either particular customers or particular IaaS providers especially since, as discussed above, complying with the verification obligations will not be particularly burdensome for customers or providers.

Question (14): The Department notes that foreign malicious cyber actors can acquire fake identities and documents and asks what the implications are for initial and ongoing customer verification requirements. Vigilantly applying verification requirements initially and on an ongoing basis is important precisely because malicious cyber actors—whether foreign or domestic—may use faked documents and lay dormant for long periods before engaging in malicious activity. Collecting and maintaining historical and current verification information—even when the customer has faked that information—can help reveal patterns. Recognizing patterns can not only aid enforcement actions after malicious activity has occurred but also help prevent additional malicious acts by the same or similar parties that rely on the same or similar faked identity information. For example, the use of "watch lists" based on information gathered from past malicious acts may help catch the same or different malicious actors at the initial verification stage, avoiding significant subsequent harm.

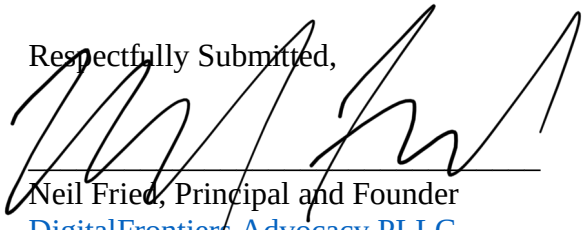
Question (15): The Department asks whether the fraud prevention regimes of other industries, such as finance, might enable more consistent discovery of the use of fake identities and documentation when verifying IaaS customers. As discussed above, the finance industry's KYC requirements provide a good template for verification requirements. Requiring customers to provide financial information would also allow providers to leverage the verification work the financial industry already does.

V. Conclusion

As policymakers seek to remedy the lack of accountability online that increasingly puts the public in harms' way, requiring internet intermediaries to verify their customers' identities presents a commonsense and non-burdensome tool. In combination with enactment of the Shop Safe Act, the Inform Consumers Act, WHOIS legislation, other Know Your Customer-type laws, and section 230 reform, as well as inclusion of online customer verification requirements in trade

agreements, such verification would go a long way toward making the internet a safer and more secure place for commerce and communication.

Respectfully Submitted,



Neil Fried, Principal and Founder
DigitalFrontiers Advocacy PLLC

Rick Lane, Child Safety Advocate
Founder and CEO, Iggy Ventures, LLC

on behalf of

1. The Alliance to Counter Crime Online
2. The Alexander Neville Foundation
3. DrugInducedHomicide.org
4. Victims of Illicit Drugs
5. The National Center on Sexual Exploitation
6. Enough Is Enough
7. Advocating Against Romance Scammers
8. Paving the Way Foundation
9. Parents Against Child Sex Abuse
10. NC Stop Human Trafficking
11. Wealth Management Ministries: Prevention Works Joint Task Force & Coalition
12. Protect Young Eyes
13. End Exploitation Montana