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"

Docket No. *DOC–2021–0007*

International Center for Law & Economics

Authored By:

Kristian Stout, Director of Innovation Policy

ICLE | 1104 NW 15th Avenue Suite 300 | Portland, OR 97209 | 503.770.0076
icle@laweconcenter.org | @laweconcenter | www.laweconcenter.org

Before the

Department of Commerce

Washington, D.C. 20554

Executive Order 13984, Taking Additional Steps To Address the National Emergency With Respect to Significant Malicious Cyber-Enabled Activities

Docket No. DOC–2021–0007

COMMENTS OF KRISTIAN STOUT, DIRECTOR OF INNOVATION POLICY, THE INTERNATIONAL CENTER FOR LAW & ECONOMICS

October 25, 2021

I. 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."[1] 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."[2]

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.[3]

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.[4] 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

---

[1] Exec. Order No. 13984, 86 C.F.R. 6837 (2021), https://www.federalregister.gov/documents/2021/01/25/2021-01714/taking-additional-steps-to-address-the-national-emergency-with-respect-to-significant-malicious.

[2] *Id.* at Sec. 1.

[3] *Taking Additional Steps To Address the National Emergency With Respect to Significant Malicious Cyber-Enabled Activities,* Advanced Notice of Proposed Rulemaking, Doc. No. DOC–2021–0007 (released Sep. 24, 2021) ("*ANPRM*"), *available at* https://www.govinfo.gov/content/pkg/FR-2021-09-24/pdf/2021-20430.pdf.

[4] See, e.g., Brandon Wiebe, *Adopting a Universal Standard for Unmasking Anonymous File Sharers*, Working Paper 2-5 (2013), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2699181.

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.

II. The law & economics of Internet anonymity

Cybersecurity breaches are not new,[5] but they have received heightened attention as the scope of hackers' ambitions has grown. In 2020, hackers infiltrated the systems of SolarWind, a developer of software to help firms manage information technology (IT) resources.[6] The hackers infected SolarWind distribution servers with malicious code that was broadcast to more than 18,000 customers.[7] The malicious code allowed the hackers to access infected machines[8] of SolarWind customers, which included both private firms and such federal agencies as the U.S. Department of Homeland Security and the U.S. Treasury Department.[9] Using similar techniques, the hackers were able to compromise other machines outside the SolarWind distribution vector.[10]

Given the scale of attacks like SolarWind, it is appropriate that policymakers seek means to enhance cybersecurity defenses. The scope of potential damage from similar future attacks should be expected to grow as more firms move more business into cloud-hosted environments using IaaS systems. And while there are many aspects to designing policy that encourages adequate cybersecurity, the EO's focus on the role of online anonymity is surely an important point on which to focus.

Extraordinary effort must be expended for an Internet user to remain fully anonymous. While there are tools designed to maximize anonymity online, computers used to access Internet-connected systems inevitably leave "fingerprints."[11] Thus,"anonymous" use of the Internet is generally better characterized as "pseudonymous." Nonetheless, for simplicity's sake, this comment will refer to such use as "anonymous."

But precisely because fully anonymous Internet use is unusual, less extreme policy interventions may achieve a great deal of positive effect. Services need not design completely foolproof user-

---

[5] *See, e.g.*, Nate Lord, *Top 10 Biggest Government Data Breaches of All Time in the U.S.*, DATAINSIDER, Oct. 6, 2020, https://digitalguardian.com/blog/top-10-biggest-us-government-data-breaches-all-time.

[6] Isabella Jibilian and Katie Canales, *The US is Readying Sanctions Against Russia Over the SolarWinds Cyber Attack. Here's a Simple Explanation of How the Massive Hack Happened and Why It's Such a Big Deal*, BUSINESS INSIDER, Apr. 15, 2021, https://www.businessinsider.com/solarwinds-hack-explained-government-agencies-cyber-security-2020-12.

[7] *Id.*

[8] *Id.*

[9] *Id.*

[10] *See, e.g.*, Marcin Kleczynski , *Malwarebytes Targeted by Nation State Actor Implicated in SolarWinds Breach. Evidence Suggests Abuse of Privileged Access to Microsoft Office 365 and Azure Environments*, MALWAREBYTES NEWS, Jan. 27, 2021, https://blog.malwarebytes.com/malwarebytes-news/2021/01/malwarebytes-targeted-by-nation-state-actor-implicated-in-solarwinds-breach-evidence-suggests-abuse-of-privileged-access-to-microsoft-office-365-and-azure-environments (Compromised Office 365 and Azure environments were being used to attempt to access sensitive emails); *see also*, Michael Sentonas, *CrowdStrike Launches Free Tool to Identify and Help Mitigate Risks in Azure Active Directory*, CROWDSTRIKE BLOG, Dec. 23, 2020, https://www.crowdstrike.com/blog/crowdstrike-launches-free-tool-to-identify-and-help-mitigate-risks-in-azure-active-directory/ (Foreign reseller tried to use compromised Microsoft services to access sensitive information).

[11] *See, e.g.*, Bhagyesh Parmar, *How to be Completely Anonymous on the Internet in 2021*, MEDIUM, May 22, 2020, https://medium.com/dsc-rngpit/how-to-be-completely-anonymous-on-the-internet-in-2020-60af1f30715e.

identification systems, but merely *sufficiently good* systems such that law enforcement or the courts are reasonably able to locate a potential defendant or suspect.

Nonetheless, it remains the case that when anonymity is combined with easily accessible tools like virtual private networks, proxy servers, and The Onion Network (Tor), it can tend to confound law enforcement.[12] And in addition to the harms that arise from anonymous use of IaaS providers, other related areas of civil and criminal law are complicated by anonymous online activity. Indeed, some of those areas may offer policy lessons for how to approach anonymity in the context of IaaS providers.

One notable example is 8chan,[13] an online forum that allowed users to interact anonymously and that styled itself as among "the Darkest Reaches of the Internet."[14] 8chan was on several occasions connected to terrorist attacks,[15] which some have attributed, in part, to the platform permitting communications in which users encouraged each other to act out in a horrific manner. In the case of an April 2019 attack on a synagogue in San Diego, for example, the perpetrator allegedly both drew inspiration for the attack from 8chan forums and used the site to advertise his actions and garner more attention from likeminded users.[16]

The perpetrator of the San Diego attack also used other services that allow anonymous interaction, such as Pastebin and Mediafire.[17] Similar sites offering free, anonymous filesharing[18] are widely available online. The perpetrator of the Christchurch, New Zealand, terrorist attack also allegedly relied on the 8chan community for support in plotting and carrying out his crime.[19] 8chan shut down briefly and resumed operations as 8kun.[20] It later faced difficulties obtaining a variety of

---

[12] *Obstacles to Cybercrime Investigations*, UNODC, https://www.unodc.org/e4j/en/cybercrime/module-5/key-issues/obstacles-to-cybercrime-investigations.html (last visited Oct. 25, 2021 12:08 PM EST).

[13] After shutting down briefly in 2019, it rebranded and relaunched as "8kun". *See*, *8chan*, WIKIPEDIA, https://en.wikipedia.org/wiki/8chan (last visited Oct. 25, 2021 12:09 PM EST).

[14] *See*, *8chan Archived Homepage*, INTERNET ACHIEVE WAYBACKMACHINE, https://web.archive.org/web/20190801063735/https:/8ch.net/index.html (last visited Oct. 20, 2021 3:52 PM EST).

[15] Georgia Wells and Ian Lovett, *'So What's His Kill Count?': The Toxic Online World Where Mass Shooters Thrive*, WALL ST. J., Sep. 4, 2019, https://www.wsj.com/articles/inside-the-toxic-online-world-where-mass-shooters-thrive-11567608631

[16] Gianluca Mezzofiore and Paul P. Murphy, *The New Zealand Mosques Attack Appeared to Inspire California Synagogue Suspect*, CNN, Apr. 29, 2019, https://www.cnn.com/2019/04/29/us/california-synagogue-8chan-new-zealand-mosque/index.html

[17] *Id.*

[18] *See, e.g.*, *Smash Homepage*, https://en.fromsmash.com/ (last visited Oct. 25, 2021 12:21 EST); *see also File Dropper,* https://www.filedropper.com/ *(last visited Oct. 25, 2021 12:46 PM EST)*

[19] Robert Evans, *Shitposting, Inspirational Terrorism, and the Christchurch Mosque Massacre*, BELLINGCAT, Mar. 15, 2019, https://www.bellingcat.com/news/rest-of-world/2019/03/15/shitposting-inspirational-terrorism-and-the-christchurch-mosque-massacre/

[20] *8kun*, https://8kun.top/index.html (last visited Oct. 25, 2021 12:49 PM EST).

infrastructure services after it was allegedly used in efforts to organize the Jan. 6, 2021, riots at the U.S. Capitol.[21]

Critically, there is no evidence that 8chan, 8kun, or its proprietors purposely cultivated or promoted terrorist activity. But the services were designed to allow the sort of anonymous interaction that may have encouraged the perpetrators of each of the foregoing examples.[22]

Less dramatically, anonymous services are frequently implicated in the piracy of copyrighted materials by criminal rings.[23] In some cases, service providers have explicitly designed their services to provide anonymity for users as a way to defeat ISP compliance with copyright law. For instance, LiquidVPN was sued earlier this year for designing and marketing its services as a "no-log" VPN.[24] LiquidVPN promoted its service as enabling use of peer-to-peer networks and pirate-streaming websites with impunity, because the company would be unable to comply with any ISP or rightsholder demands to unmask users.[25] Economists Jian Jia and Liad Wagman have similarly noted that choices by platforms like Airbnb to preference user pseudonymity can make it difficult to enforce short-term-rental laws.[26]

There are other examples of online services, however, that changed their policies when confronted with unlawful activity by anonymous or otherwise difficult-to-locate users. These examples illustrate the value of a nuanced approach to user anonymity online.

In 2020, MindGeek—a pornography conglomerate that operates sites such as PornHub and YouPorn—lost access to credit-card-processing services from Visa and Mastercard for allegedly allowing child sexual abuse materials (CSAM) to proliferate on its sites.[27] In response to the

---

[21] Kari Paul, Luke Harding and Severin Carrell, *Far-right Website 8kun Again Loses Internet Service Protection Following Capitol Attack*, THE GUARDIAN, Jan. 15, 2021, https://www.theguardian.com/technology/2021/jan/15/8kun-8chan-capitol-breach-violence-isp

[22] Of course, user anonymity is not the only reason sites like 8chan may become hotbeds for organizing this sort of activity. The site's lack of moderation is a very important factor. Sites like Twitter and Facebook, with relatively less anonymity than 8chan, would almost certainly see more illicit use of their services but for their massive investments in content moderation. Nonetheless, at the margins, an environment that cultivates maximal anonymity is more likely to provide an environment in which this sort of activity is the norm.

[23] For example, in a recent English case, the High Court found that it was legally appropriate to an issue an order to Internet service providers to block operators of "cyberlockers" that are used to anonymously store and share pirated digital media files. Capitol Records, et al. v. British Telecommunications PLC et al., 2021 EWHC 409 para. 25 (2021) (England and Wales High Court Chancery Division), *available at* https://www.bailii.org/ew/cases/EWHC/Ch/2021/409.html

[24] See Alyse Stanley, *LiquidVPN Faces Lawsuit for Allegedly Promoting Pirating Content*, GIZMODO, Mar. 4, 2021, https://gizmodo.com/liquidvpn-faces-lawsuit-for-allegedly-promoting-piratin-1846412019; *see also* Liquid*VPN sued by film studios*, TECHTYPICAL, Sep. 29. 2021, https://www.techtypical.com/news/liquidvpn-lawsuit/

[25] *Id.*

[26] Jian Jia & Liad Wagman, *Platform, Anonymity, and Illegal Actors: Evidence of Whac-a-Mole Enforcement from Airbnb*, 63 J.L. & ECON. 729, 730 (2020). Importantly, this is not a defense of those short-term-rental laws, which one could reasonably conclude are special-interest protections for hotels and motels that harm consumer welfare. But the answer to bad laws is to repeal them, not to create an indiscriminate loophole that makes good and bad laws alike harder to enforce.

[27] Samantha Cole, *Visa and Mastercard Will Stop Processing Payments to Pornhub*, VICE, Dec. 10, 2020, https://www.vice.com/en/article/7k94be/mastercard-will-stop-processing-payments-to-pornhub.

allegations, MindGeek took down a large volume of material, leaving up only that content created by users with *verified* accounts.[28] Thus, to avoid hosting an unacceptable amount of illegal content, MindGeek adopted a moderation method that would permit user deanonymization.

This makes sense in at least two ways. First, if law enforcement identifies a legitimate target that uploads CSAM, MindGeek can provide information that furthers an investigation. Second, having a policy requiring verified identities deters the marginal user who might otherwise be interested in using MindGeek's platform to distribute CSAM. That is to say, an identity-verification scheme can make a potential criminal think twice before uploading CSAM.

Amazon was also forced to come to terms with difficult-to-locate merchants that sell on its platform. In *Oberdorf v. Amazon*, a woman lost sight in one eye because of a defective product sold by a third-party merchant on Amazon.com.[29] The seller of the defective merchandise subsequently disappeared.[30] Amazon was ultimately found liable under Pennsylvania products-liability law, because it designed its system in such a way that users could not reliably contact third-party sellers.[31]Although Amazon never publicly announced changes to its services as a response to *Oberdorf*, over the last year or two, it did begin to require more detail and additional steps in its merchant-verification process that would weed out fraudulent sellers.[32] Relatedly, as counterfeit products have become a growing problem for Amazon,[33] it has devoted greater resources to its brands-registry program, which works to validate that third-party merchants are entitled to sell identified brand-name goods.[34]

In the context of Section 230 of the Communications Decency Act, Professor Gus Hurwitz has proposed changes that would make the law's immunity shield contingent on platform operators' ability to deanonymize users:

> To wit, Section 230's immunity could be attenuated by an obligation to facilitate the identification of users on that platform, subject to legal process, in proportion to the size and resources available to the platform, the technological feasibility of such identification, the foreseeability of the platform being used to facilitate harmful speech

---

[28] *Visa Reinstates Card Use On Some MindGeek Sites, Pornhub Still Banned*, PYMNTS, Dec. 23, 2020, https://www.pymnts.com/visa/2020/visa-reinstates-card-use-some-mindgeek-sites-pornhub-still-banned/

[29] *See* Oberdorf v. Amazon.com Inc., 930 F.3d 136 (3d Cir. 2019).

[30] *See id.* at 142.

[31] *See id.* at 153-54.

[32] *See, e.g.*, Nicolas Vega, *New Amazon Sellers Now Have to Verify Their Identities Over Video Chat*, NEW YORK POST, Apr. 27, 2020, https://nypost.com/2020/04/27/amazon-making-new-sellers-verify-identity-over-video-chat/

[33] *See, e.g.*, Chaim Gartenberg, *Amazon Launches Counterfeit Crimes Unit to Fight Knockoffs on its Store*, THE VERGE, June 24, 2020, https://www.theverge.com/2020/6/24/21302114/amazon-counterfeit-crimes-unit-knockoffs-store-online-investigators.

[34] *See Amazon Brand Registry*, Amazon.com, https://brandservices.amazon.com/ (last visited Oct. 25, 2021 1:33 PM EST).

> or conduct, and the expected importance (as defined from a First Amendment perspective) of speech on that platform.[35]

The core insight of this proposal—and of the general observation that firms should be required to be able to identify customers when necessary to comply with law-enforcement ends—is that the law is frequently used to assign liability and other obligations on intermediaries when they are least-cost avoiders.[36] An important goal of the law is to align individual incentives with social welfare such that costly behavior is deterred and individuals are encouraged to take optimal levels of precaution against risks of harm.

Typically, a least-cost avoider incurs some liability as an intermediary for failing to prevent a foreseeable harm; but the same concept applies to imposing additional legal obligations on a firm when those obligations facilitate legal process. In this sense, where the magnitude of harms from anonymous use of IaaS providers is sufficiently large, placing additional legal compliance burdens to adequately verify users can, on net, generate the least overall social cost. In terms of the classic Learned Hand formula, where the probability of a harm (p) times the magnitude of that harm (L) is sufficiently high, and the cost of verification (B) sufficiently low (thus, $B < pL$), the precaution of requiring user verification is justified.[37]

The ultimate objective in imposing a deanonymization obligation on service providers is to facilitate the optimal level of law enforcement, while not unduly interfering with the operation of private firms.

A. Know your business customer

Relevant to the questions presented in this ANPRM is how different jurisdictions and scholars have conceptualized and implemented these ideas in the context of "know your business customer" (KYBC) policies. These policies take various forms. Financial services firms, for example, long have faced obligations to obtain and verify certain customer information, in concert with efforts to curb money laundering and other financial crimes.[38]

---

[35] Gus Hurwitz, *The Third Circuit's Oberdorf v. Amazon Opinion Offers a Good Approach to Reining in the Worst Abuses of Section 230*, TRUTH ON THE MARKET, July 15, 2019, https://truthonthemarket.com/2019/07/15/the-third-circuits-oberdorf-v-amazon-opinion-offers-a-good-approach-to-reining-in-the-worst-abuses-of-section-230/.

[36] A "least-cost avoider" is a person or other entity involved in a legally relevant situation who is best positioned to deter certain harmful conduct at least overall cost. *See* Harold Demsetz, *When Does the Rule of Liability Matter?*, 1 J. OF LEG. STUD. 13, 28 (1972). *See generally* Ronald Coase, *The Problem of Social Cost*, 3 J. L. & ECON. 1 (1960).

[37] *See United States v. Carroll Towing Co.*, 159 F.2d 169 (2d Cir. 1947).

[38] *See, e.g.*, Customer Due Diligence Requirements for Financial Institutions, 81 FR 29397 (2016) (requiring financial institutions to begin collecting information on the beneficial ownership of corporate entities).

EU governing bodies currently are considering KYBC requirements as a means to mitigate the impediments to law enforcement posed by anonymous users of Internet platforms.[39] Under the EU's approach, intermediaries would be required to record and verify the identity of their business customers.[40] Thus, platform users would be able to remain generally anonymous to other users, but if they engage in illegal conduct, their identities would be made known to law enforcement. This approach could enable law enforcement to pursue parties responsible for illegal behavior directly, with minimal burden on the platforms and their non-business customers.

The EU proposal has been promoted alongside the use of "known business" registries as a verification mechanism that can provide real contact information to aggrieved parties when harm occurs.[41] Until recently, there has been a paucity of effective global solutions for identity verification due to the absence of available registries and the cost of operating identity-verification systems.[42]

Increasingly, however, new solutions are being made available. Both public and private-sector secure digital identity registries are in development.[43] According to the World Bank, 161 countries now have digital identity systems, although many are very basic.[44] New systems that use distributed-ledger technologies to establish connections with trusted networks of identity-verification providers could dramatically reduce the risk of data breaches by storing information pseudonymously and sharing only limited information.[45] Thus, as the technology to manage identity-verification proliferates, the costs of accessing such technology are likely to fall such that access to the technology does not create a barrier to competition.

III. Conclusion and recommendations

Any rules implemented under the EO should have the goal of being to obtain reasonable compliance, such that as much illegal activity as possible is deterred without unnecessarily burdening

---

[39] Jan Bernd Nordemann, *The Functioning of the Internal Market for Digital Services: Responsibilities and Duties of Care of Providers of Digital Services*, IMCO committee, EU Parliament (2020), *available at* https://www.europarl.europa.eu/RegData/etudes/STUD/2020/648802/IPOL_STU(2020)648802_EN.pdf

[40] *Id.* at 54-55

[41] *Id.* at 11

[42] Indeed, there is a great deal of risk involved in operating centralized registries, as evidenced by the Equifax data breach. *See* Josh Fruhlinger, *Equifax Data Breach FAQ: What Happened, Who Was Affected, What Was the Impact?*, CSO, Feb. 12, 2020, https://www.csoonline.com/article/3444488/equifax-data-breach-faq-what-happened-who-was-affected-what-was-the-impact.html.

[43] Bryan Pon, Chris Locke, and Tom Steinberg, *Private-Sector Digital Identity in Emerging Markets*, Caribou Digital (2016), *available at* https://www.cariboudigital.net/wp-content/uploads/2019/01/Caribou-Digitial-Omidyar-Network-Private-Sector-Digital-Identity-In-Emerging-Markets.pdf

[44] *ID4D Data: Global Identification Challenge by the Numbers*, The World Bank, https://id4d.worldbank.org/global-dataset (last visited Oct. 25, 2021 2:01 PM EST)

[45] Shu Yun Lim, Pascal Tankam Fotsing, Abdullah Almasri, and Omar Musa, *Blockchain Technology the Identity Management and Authentication Service Disruptor: A Survey*, 8(4-2) INT'L J. ADVANCED SCIE. ENGINEERING & INFO. TECH. 1735 (2018), *available at* https://www.researchgate.net/publication/328919940_Blockchain_Technology_the_Identity_Management_and_Authentication_Service_Disruptor_A_Survey

the firms and their customers. The ANRPM asks whether "commenters believe that the Department should place more emphasis on ongoing customer-due-diligence efforts instead of initial Account creation requirements[.]"[46] Surely, having an initial set-up requirement is important, but so too is some obligation to periodically re-verify customer information.

But the issue is not whether one or the other is more effective, as both are elements of ongoing reasonable behavior. The key question, rather, is how extensive the requirements should be, and how much reliance is placed upon the IaaS providers as a cornerstone of law enforcement. The effort that a provider can put into verifying the identity of its customers will necessarily be limited, while dedicated criminals will find ways around every set of legal obstacles. Thus, the requirements should be designed to obtain the optimal amount of information that law enforcement and courts need *in most, but not all, cases.* It is likely that a minimal set of requirements and an ongoing obligation to re-verify identities will resolve most problems associated with anonymous users.

The ANPRM asks "[h]ow might a framework for best practices account for the dynamic and ever-evolving threat environment while allowing U.S. IaaS providers to stay agile in their company-specific programs?"[47] In general, it would be best to avoid overly prescriptive regulations beyond requirements that providers maintain records sufficient to identify bad actors in most cases. Moreover, it would be highly inadvisable to prescribe specific technological measures or programs that providers must use—the history of the last 20 years demonstrates that technology inevitably moves faster than regulation. Therefore, providers should be free to implement identity-verification systems as they see fit, so long as those systems are capable of eliciting the needed information.

The ANPRM asks "[s]hould exemptions be granted on a one-time basis, or should such exemptions be time-limited, with an obligation of renewal after a certain period of time?"[48] This question centers on how best to design defaults: should we expect that there are classes of business activity that deserve permanent exemption from a default rule that businesses maintain some minimal amount of information on their customers? If the nature of IaaS services is such that the relationship between provider and customer is likely to change in important ways in a relatively short time frame, then exemptions should be appropriately limited. If the Secretary is unsure as to which set of defaults is appropriate, perhaps drawing on lessons from other analogous areas of law and regulation would be useful.

One potentially useful example is the triennial review process for exemptions from Section 1201 of the Digital Millennium Copyright Act overseen by the Librarian of Congress.[49] The purpose of that process is to permit users to bypass "technological protection measures" that otherwise are used to

---

[46] ANPRM, *supra*, note 3 at para. 14.

[47] *Id.* at para. 5(d).

[48] *Id.* at para. 5(a).

[49] *See generally The Triennial Rulemaking Process for Section 1201*, United States Copyright Office, https://cdn.loc.gov/copyright/1201/1201_rulemaking_transcript.pdf (last visited Oct. 25, 2021 2:12 PM EST).

protect copyrighted material.[50] Every three years, the Librarian of Congress reconsiders existing exemptions and considers new exemptions.[51] Familiarity with the triennial review process could help to demonstrate the practicality of designing exemptions to the verification rules.[52]

The Department is further interested in thoughts on how to ensure compliance, and when to verify compliance. Specifically, it asks "[w]hat should the Department consider when deciding how compliance with the requirements adopted under Section 1 should be monitored and enforced (*i.e.*, should compliance and enforcement be strictly limited to instances following malicious cyber activities that are traced back to specific U.S. IaaS providers; should the Department implement a voluntary or required proactive suspicious/abnormal Account activity report mechanism to assist in ongoing due diligence; should the Department periodically conduct compliance audits)?"[53] Again, the goal of these regulations should be to achieve optimal information on bad actors with the least amount of interference in the operations of firms subject to the requirements.

This is not just to avoid creating excessive compliance burdens, but to avoid imposing on the Department oversight duties that could quickly become unmanageable, or that degrade into mere security theater in the face of a huge volume of customer accounts at IaaS providers. Indeed, most user accounts on IaaS services will be of no interest at all to the Department, and it is those users who have the most incentive to comply with requirements that they disclose accurate information. So long as subject firms are minimally compliant, determining the sufficiency of their identity-verification activities will inevitably be an *ex post* procedure.

With that said, encouraging firms to work together, and in conjunction with the Department, to develop a *voluntary* proactive-monitoring system for suspicious activities on their services is, on the whole, likely to do more good than harm.

Finally, the ANPRM asks about the potential international consequences of imposing these obligations.[54] Relatedly, the ANPRM also asks "how might the European Union General Data Protection Regulation (GDPR), the California Consumer Privacy Act (CCPA), or other relevant data protection and security laws and regulations affect U.S. IaaS providers' ability to fulfill these record- keeping requirements pursuant to E.O. 13984?"[55]

The Department is correct to acknowledge that compliance with laws like the GDPR could become a major issue for IaaS providers also subject to requirements pursuant to the EO. Indeed, other

---

[50] *Id.* at slide 4.

[51] *Id.*

[52] Note, I am not suggesting the triennial review process as a perfect model to emulate. It certainly has its critics. Instead, if the Secretary is considering a system of exemptions, I merely suggest that reviewing the Library of Congress's experience with administering a similar exemption scheme may be informative.

[53] ANPRM, *supra*, note 3 at (j)(4).

[54] *Id.* at (j)(3).

[55] *Id.* at (j)(2).

identity-verification systems had to be changed in the wake of the GDPR. For instance, ICANN, the organization that manages the worldwide domain-name system, maintains a form of identity registry called "WHOIS."[56] The WHOIS information on domain owners can be used, among other things, in service of process when the websites operating under the domain name are involved in illegal activity. Currently, the WHOIS information that domain-name providers collect ranges from accurate and capable of identifying parties when necessary[57] to anonymized, such that it is difficult to serve legal process on the owner of the domain.[58]

After the GDPR was passed, however, it became more difficult to access WHOIS information. In response to the GDPR, ICANN adopted the "Temporary Specification for gTLD Registration Data"—which, among other things, ensures that ICANN's WHOIS database complies with the GDPR.[59] In essence, GDPR compliance entails redacting from easy public access any personally identifiable information of domain owners.[60] This adds additional burdens on courts and law-enforcement officials seeking to unmask domain owners potentially engaged in criminal activity.

For the purposes of this ANRPM, it is important that firms are allowed to shape their identity-verification systems in ways that comply with the GDPR. This further underscores the above-noted need to refrain from prescribing specific technological requirements or methods, but instead to focus on the goal of enabling sufficient access to customer information when legally necessary.

Notwithstanding the above caveats, the Department is pursuing a sound policy by instituting KYBC requirements on IaaS providers. Ultimately, the question is not whether to adopt such a policy, but how best to do so. Understanding that no system will be perfect, and that the vast amount of IaaS providers' customer relationships should continue relatively unburdened, the Department's final rules should capture *most* bad actors by relying on obligations to supply minimal, but sufficient, user information.

---

[56] *About WHOIS*, ICANN, *available at* https://whois.icann.org/en/using-whois (last visited Oct. 25, 2021 2:16 PM EST).

[57] *ID check*, .dk hostmaster, https://www.dk-hostmaster.dk/en/id-check (last visited Oct. 25, 2021 2:18 PM EST).

[58] *Immaculate Release*, Njalla, Apr. 19, 2017, https://njal.la/blog/opening/ (last visited Oct. 25, 2021 2:19 PM EST).

[59] *Data Protection/Privacy Issues*, ICANN, https://www.icann.org/dataprotectionprivacy (last visited Oct. 25, 2021 2:20 PM EST).

[60] Anthony Eden, *GDPR and WHOIS Privacy*, DNSIMPLE, Apr. 3, 2019, https://blog.dnsimple.com/2019/04/gdpr-and-whois-privacy/.