CENTER FOR DEMOCRACY & TECHNOLOGY

April 29, 2024
Via email IaaScomments@bis.doc.gov

Re: NPRM on Taking Additional Steps To Address the National Emergency With Respect to Significant Malicious Cyber-Enabled Activities, DOC–2021–0007

This comment is submitted on behalf of the Center for Democracy & Technology (CDT), a non-partisan, non-profit organization that works to promote democratic values by shaping technology policy and architecture, with a focus on the rights of the individual. For over a quarter century, CDT has worked to protect the privacy of electronic communications content and metadata against unwarranted government access.

We appreciate the opportunity to comment on the notice of proposed rulemaking proposing further steps to address malicious cyber-enabled activities (NPRM).[1] The NPRM was issued under the authority of Executive Orders 13984[2] and 14110,[3] as well as the International Economic Powers Act (IEEPA).[4] We generally support the goal of the Department of Commerce (DOC) to prevent foreign actors from exploiting U.S.-based infrastructure providers to facilitate malicious cyber activity.

However, the portion of the proposed rule that requires the reporting of subscriber information and transactional records to DOC would, if complied with, compel violations of the Stored Communications Act (SCA). In short, the NPRM would require, in limited circumstances, Infrastructure as a Service (IaaS) providers that are covered by the SCA to report subscriber information and transactional records to the DOC. That requirement would fail to account for the requirement of the SCA that governmental entities seeking such information must first obtain a subpoena, court order or warrant.

The proposed rule would also require all IaaS providers to collect sensitive information from users that raise significant privacy concerns and that could make IaaS providers attractive targets for malicious actors. DOC should alter its proposal to mitigate those privacy concerns.

---

[1] Notice of Proposed Rulemaking, Department of Commerce, Taking Additional Steps to Address the National Security Emergency with Respect To Significant Malicious Cyber-Enabled Activities, Docket No. DOC–2021–0007 (Jan. 29, 2024). https://www.federalregister.gov/documents/2024/01/29/2024-01580/taking-additional-steps-to-address-the-national-emergency-with-respect-to-significant-malicious.

[2] Taking Additional Steps to Address the National Emergency With Respect to Significant Cyber-Enabled Activities (Jan. 19, 2021), https://www.federalregister.gov/documents/2021/01/25/2021-01714/taking-additional-steps-to-address-the-national-emergency-with-respect-to-significant-malicious.

[3] Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence (Nov. 1, 2023), https://www.federalregister.gov/documents/2023/11/01/2023-24283/safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence.

[4] 50 USC Section 1701 et seq.

CENTER FOR DEMOCRACY & TECHNOLOGY

I. The NPRM

The NPRM would require U.S. IaaS providers and foreign resellers of their services to maintain Customer Identification Programs (CIPs) that enable the IaaS provider to ascertain the true identity of each foreign customer and their beneficial owners, including whether they are U.S. persons. The NPRM defines IaaS as, "a product or service offered to a consumer … 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." The consumer of the service could be an individual or a business — the proposed rule would require the IaaS provider to collect identifying information regardless. Each time a customer attempts to open an account with the IaaS provider, the provider must ask it to provide the information necessary to support any assertion that the company or individual opening the account is a U.S. person.

The record keeping requirements that would be imposed on IaaS providers with respect to their prospective non-U.S. person account holders and, in the case of foreign businesses, their beneficial owners, are exacting and specific. They must include name, address, email address, account number, credit card number used for payment, virtual currency wallet or wallet address identifier used for payment, telephone number, IP address used for access and the date and time of each such access of the account.

In addition to the record keeping requirements, Section 7.308 of the proposed rule requires that IaaS providers report detailed customer and transactional information whenever they have knowledge of a "transaction by, for, or on behalf a foreign person which results or could result in the training of a large [artificial intelligence] model with potential capabilities that could be used in malicious cyber-enabled activity."[5]

II. Compelled Disclosure Requirements of the Rule Must Conform To the SCA

The compelled disclosure requirements in Section 7.308 of the proposed rule do not account for privacy protections in the SCA. Entities that are IaaS providers under the proposed rule will usually also be providers of "remote computing services" to the public (RCS providers) under the SCA, which protects the privacy of the customer records they hold. The SCA defines a "remote computing service" as "the provision to the public of computer storage or processing services by

[5] These large AI models are defined in the proposed rule as, "any AI model with the technical conditions of a dual-use foundation model or otherwise has technical parameters of concern, that has capabilities that could be used to aid or automate aspects of malicious cyber-enabled activity, including but not limited to social engineering attacks, vulnerability discovery, denial-of-service attacks, data poisoning, target selection and prioritization, disinformation or misinformation generation and/or propagation, and remote command-and-control of cyber operations. A model shall be considered to be a large AI model with potential capabilities that could be used in malicious cyber-enabled activity under this definition if it meets the technical conditions described in interpretive rules issued by the Department and published in the **Federal Register**. [Emphasis in the original]. These interpretive rules have not yet been issued.

means of an electronic communications system."[6] This definition of RCS in the SCA is very similar to the definition of IaaS provider in the proposed rule, which encompasses entities that provide "processing, storage … or other other fundamental computing resources" to consumers. Many companies that are IaaS providers under the NPRM will also be RCS providers under the SCA.

IaaS providers that are also RCS providers under the SCA must follow the SCA's restrictions on disclosure to governmental entities, such as the Department of Commerce. The SCA requires governmental entities to obtain a subpoena, court order, or warrant to compel an RCS to disclose "subscriber information" unless an exception to this requirement applies.[7] The exceptions, which cover circumstances such as emergencies[8] and consent, do not apply.

Subscriber information that the SCA protects includes name, address, means of payment, and other customer information that mirrors what the proposed rule would require an IaaS provider to report affirmatively when it obtains knowledge that a foreign IaaS customer is planning to train a large AI model.[9] The SCA bars RCS providers from making the disclosures that the proposed rule would require in the absence of appropriate legal process.[10] Even if IEEPA could authorize a disclosure rule in the absence of the SCA, its general provisions cannot trump a detailed and specific statutory requirement such as that contained in the SCA.[11]

The proposed rule's compelled disclosure provision would appear to cast a broad net due its vague terminology about "potential capabilities that could be used," and its breadth, encompassing potential use of a large model in "malicious cyber-enabled activity." Models that assist in coding software–both large and small, closed and open source–are already widely available. These models can already be used to create software tools for detecting and exploiting software vulnerabilities. For example, Microsoft and OpenAI have already observed "attackers

[6] 18 USC 2711(2).
[7] 18 USC 2703(c)(2).
[8] Although the NPRM is issued under the authority of the International Emergency Economic Powers Act (IEEPA), the circumstances under which IaaS providers serve foreign customers would not amount to an emergency under the SCA, which requires an imminent risk of death or serious bodily harm. 18 USC 2702(c)(4).
[9] The proposed rule would require disclosure to the DOC of the name, address, email address, account number, credit card number used for payment, virtual currency wallet or wallet address identifier used for payment, telephone number, IP address used for access, and the date and time of each such access of the account. The proposed rule would also require disclosure of information about the training run and cybersecurity practices relating to such training run.
[10] For much of the information, the government would need at least a subpoena. The IP address records the proposed rule requires IaaS providers to disclose may be protected by the SCA's court order requirement — a subpoena would not do.
[11] Robert S. Litt and Richard Salgado, "The Commerce Department's Stored Communications Act Problem," Lawfare, April 23, 2024. Litt, the former General Counsel of the Office of the Director of National Intelligence, and Salgado, a former official in the Computer Crimes and Intellectual Property Section of the Department of Justice and former Director of Law Enforcement and Information Security at Google, have extensive experience in exactly these issues.

using AI as another productivity tool on the offensive landscape" and making "incremental" advances in capability thanks to large language models.[12]

Therefore the capabilities of current large models would already seem to meet the amorphous standard of "potential capabilities" that "could" be used for malicious cyber activity. To the extent the NPRM also compels disclosure of customer information when an IaaS provider gains knowledge of a transaction relating to AI models that can aid in or automate "disinformation or misinformation generation and/or propagation" and "social engineering attacks," then it also would appear to extend to generative AI models that don't even have the capability to code software but simply can generate synthetic text and imagery (i.e., almost all of them). Indeed, it is not clear what size or type of large AI model would *not* have "potential capabilities" that "could be used" for malicious cyber-enabled activities, such that any foreign person seeking to use enough compute to train any large model could potentially have their information disclosed to the government under the proposed rule.

Although the DOC cannot require disclosure of customer information as a matter of course by rule, the SCA does provide for disclosure to the government with the appropriate predicate. Under the SCA, subscriber information can be compelled with a subpoena in a criminal investigation or through an available administrative subpoena.[13] It could also be compelled from an RCS provider with a national security letter (NSL) to seek information relevant to an investigation to protect against international terrorism or clandestine intelligence activities.

The Commerce Department should drop the compelled disclosure provisions in Section 7.308 of the proposed rule, or limit such requirements to entities that are not covered by the Stored Communications Act. If it does not, it should explain in detail how such compelled disclosure of customer information comports with the SCA.

III. Record Keeping Requirements Must Protect User Privacy

Unlike the disclosure provisions in proposed Section 7.308, the record keeping requirements of the NPRM do not raise concerns about legality under the SCA . But, they do raise significant privacy concerns regarding the data of both U.S. persons and non-U.S. persons who use IaaS services.

The NPRM proposes a rule that would require IaaS providers to adopt Customer Identification Programs that enable them to distinguish their U.S. person users from their non-U.S. person users. It invites them to use documentary and non-documentary means for doing so, but does not specify what those means might be.

---

[12] Microsoft Threat Intelligence, "Staying Ahead of Threat Actors in the Age of AI," Microsoft Security Blog (blog), February 14, 2024, https://www.microsoft.com/en-us/security/blog/2024/02/14/staying-ahead-of-threat-actors-in-the-age-of-ai.

[13] 18 USC 2703(c)(2).

Generally, a U.S. person is an individual who is either a U.S. citizen or a lawful permanent resident of the U.S., also known as a "green card" holder. Documentary evidence of U.S. person status that one might be required to provide could be inferred from the types of documents that the U.S. Citizenship and Immigration Services requires employers to examine to confirm authorization to work in the United States.[14] The documents that prove such status are quite limited: a U.S. passport, a U.S. green card and possibly a birth certificate.[15] Because non-U.S. persons visiting the U.S. can obtain driver's licenses and state identification cards,[16] such documents cannot establish U.S. person status. Non-documentary methods to verify U.S. person status may also be used, but what they might be are not spelled out in the proposed rule. As a result, the NPRM encourages or effectively requires IaaS providers to demand documentary evidence from their users as part of their Customer Identification Programs.

Further, the IaaS provider is required to verify the authenticity of these documents, but the NPRM does not say how they should do that. Because IaaS providers will need to be able to show that they authenticated documentary evidence (including when they are audited to ensure compliance) or face penalties for failure to do so, many will retain copies of the documentary evidence submitted by people who claim to be U.S. persons. This creates a significant concern about the privacy of U.S. persons who use IaaS services. They can include people particularly vulnerable to abuse, such as journalists, dissidents, and business people who frequently travel abroad. The rule the DOC issues should recognize this privacy risk to U.S. persons, specify the documentary and non-documentary evidence that would be acceptable to verify U.S. person status, and indicate specifically that a Customer Identification Program that meets the requirements of the rule must include prompt destruction of such documentary evidence after U.S. person status is verified.

The privacy risk that the NPRM poses to non-U.S. persons is greater than the risk it poses to U.S. persons because it requires retention of sensitive personal information for two years after the account is closed or was last accessed. Information about an IaaS customer that must be retained includes name, address, email address, account number, credit card number used for payment, virtual currency wallet or wallet address identifier used for payment, telephone number, IP address used for access and the date and time of each such access of the account. The purpose of this lengthy and intrusive data retention requirement is to facilitate prosecution of foreign persons who use IaaS services for malicious purposes.

The proposed data retention requirements with respect to non-U.S. persons who seek to use U.S. IaaS products and services seem disproportionate to the risk of abuse of those services

[14] USCIS Form I-9 Acceptable Documents, https://www.uscis.gov/i-9-central/form-i-9-acceptable-documents.
[15] According to USCIS, a birth certificate can establish work authorization, but not identity.
[16] U.S. Immigration and Customs Enforcement, "Applying for a Driver's License or State Identification Card," https://www.ice.gov/doclib/sevis/pdf/dmv_factsheet.pdf.

because they apply to all non-U.S. persons. They are inconsistent with data minimization best practices and they create an attractive target — the IaaS provider — for some of the types of malicious cyberattacks that the NPRM aims to prevent or discourage. They are also inconsistent with the data minimization requirements of the European Union's GDPR, which in many circumstances require companies to delete personal data that is not in use.

The DOC should reconsider the data retention requirements it would impose on IaaS providers serving non-U.S. persons with an eye toward requiring retention of a more limited data set for a more limited period of time. If it does not do so, non-U.S. persons may look elsewhere for IaaS services (harming the competitiveness of U.S. companies) and may utilize services that are less secure than those that may be offered by U.S. IaaS providers, posing an even greater risk of malicious use.

IV. Conclusion

CDT supports the DOC's goal in this proceeding of preventing foreign actors from exploiting U.S.-based infrastructure providers to facilitate malicious cyber activity. We urge the DOC to conform the compelled disclosure requirements in the final rule to the SCA and to take steps to account for the privacy interests of both U.S. person and non-U.S. person consumers of IaaS products and services when crafting the record keeping requirements of the final rule.

Please address any questions about this comment to Gregory Nojeim, Director of the CDT Security and Surveillance Project, at gnojeim@cdt.org.