NOTICE OF PROPOSED RULEMAKING DOCKET NO. NSD-104
AG ORDER NO. 6067-2024; RIN 1124-AA01
89 FR 86116 (Oct. 29, 2024)

DEPARTMENT OF JUSTICE: PROPOSED RULE ON PROVISIONS PERTAINING TO PREVENTING ACCESS TO U.S. SENSITIVE PERSONAL DATA AND GOVERNMENT-RELATED DATA BY COUNTRIES OF CONCERN OR COVERED PERSONS

MEETING SUMMARY

RE: MEETING WITH THE INFORMATION TECHNOLOGY INDUSTRY COUNCIL ("ITI") REGARDING THE DEPARTMENT OF JUSTICE'S PROPOSED RULE ON PROVISIONS PERTAINING TO PREVENTING ACCESS TO U.S. SENSITIVE PERSONAL DATA AND GOVERNMENT-RELATED DATA BY COUNTRIES OF CONCERN OR COVERED PERSONS

DATE/TIME OF MEETING: November 26, 2024 11:30 AM – 12:00 PM EST

PLACE OF MEETING: VIRTUAL

ATTENDEES:

FROM THE NATIONAL SECURITY DIVISION OF THE DEPARTMENT OF JUSTICE

Allison Harrington, Attorney
Jailene Acevedo, Paralegal
Jennifer Roan, Program Analyst
Joe Bartels, Attorney
Kaveh Miremadi, Attorney
Lee Licata, Deputy Chief for National Security Data Risk

FROM THE DEPARTMENT OF COMMERCE

Isabella Carlton, Policy Advisor, Global Data Policy and Privacy
Marvin Wiley, Policy Advisor, Global Data Policy and Privacy

FROM THE CYBERSECURITY AND INFRASTUCTURE SECURITY AGENCY

Peter Colombo, Deputy Section Chief

FROM THE INFORMATION TECHOLOGY INDUSTRY COUNCIL

Coutrney Lang, Vice President of Policy, Trust, Data, and Technology
John Miller, Senior Vice President and General Counsel
Sameer Boray, Senior Manager of Policy, Trust, Data, and Technology

SUMMARY OF MEETING:

On November 26, 2024, representatives from the Department of Justice ("DOJ") and the Commerce Department ("Commerce") engaged with representatives from The Information Technology Industry Council ("ITI") regarding ITI's comments on DOJ's October 29, 2024 Notice of Proposed Rulemaking ("NPRM") entitled "Proposed Rule on Provisions Pertaining to Preventing Access to U.S. Sensitive Personal Data and Government-Related Data by Countries of Concern or Covered Persons." *See* 89 FR 86116. These notes are a summary of the engagement; they are not a transcript. The Department of Justice has not shared these notes with meeting participants to confirm their accuracy.

During the engagement, a representative from DOJ briefly discussed the NPRM's proposed requirements, including exceptions to the proposed rule, changes from DOJ's March 5, 2024 Advanced Notice of Proposed Rulemaking ("ANPRM"), and comments received on the ANPRM. *See* 89 FR 15780. DOJ also noted that the NPRM comment period is open until November 30, 2024, and encouraged participants to submit comments on the proposed rule. During the engagement, representatives from DOJ also invited meeting participants to ask questions about the NPRM from participants.

Commerce asked that ITI describe their role in industry and present any concerns they have pertaining to DOJ's NPRM. ITI stated that they represent 80 of largest global technology companies, including hardware manufacturers and AI companies. They specified that approximately 60-70% to headquartered in the United States and others in Europe and Asia.

In response to Commerce, ITI stated that their comment on DOJ's NPRM would be posted on Wednesday, November 27th.

Commerce asked if ITI had concerns on the proposed rule, particularly economic impact, compliance, data transactions, or bulk thresholds.

ITI's first concern is with the economic impact of the proposed rule. ITI believes that DOJ's cost estimates are a slightly narrow, with some of their companies concerned that the cost to comply will be higher. ITI added that an indirect cost could be reduced U.S. global competitiveness resulting from foreign competitors obtaining market share. They added that economic competitiveness and national security are interconnected.

DOJ asked ITI how, specifically, the companies that believe compliance would cost more than DOJ assessed would incur said higher costs. DOJ asked that ITI provide examples of what would be more expensive in order to be in compliance with the proposed rule.

ITI replied that all their companies have existing and operational global privacy programs for compliance. They stated that proposed rule would cause them to create duplicative processes for record keeping and auditing. ITI's represented companies are concerned with how the proposed rule integrates into existing data governance compliance programs.

DOJ asked that if ITI companies already comply with existing privacy regimes, such as GDPR and if many of the rules requirements are duplicative of that type of regime, what part of

or requirement in the proposed rule would increase compliance costs in an unanticipated manner?

ITI explained that under GDPR, companies must already conduct transfer risk assessments, among other security measures associated with transfers. Some of these requirements overlap with those in the proposed rule whereas others do not.

DOJ asked ITI what type of sensitive information is not normally regulated under GDPR but is covered under the proposed rule. ITI replied stating that the "covered personal identifiers" category and added that such identifiers are critical to their companies' operation. In addition, ITI believes that this aspect of the proposed rule intersects with decision to include rather than exclude pseudonymized data from the scope of the rule. ITI also raised concern as to whether these types of identifiers can actually be used to identify a person and create a national security risk.

DOJ asked if ITI's challenge with the proposed rule is not the identifiers themselves but having to assess the combinations of personal identifiers identified in the rule. DOJ clarified that there are 3 categories of CPI all of which require some combination of identifiers or identifiers and other bulk sensitive personal data to be linked or linkable to an individual. DOJ also asked ITI if their companies would be more comfortable if all PII, to include these identifiers, instead was regulated as opposed to combinations of identifiers. ITI stated that they would be unable to answer these questions unless their view was substituted for that of each company. Given the variety of companies they represent, ITI stated that it would be difficult to provide answers to the above.

ITI added, nonetheless, that their companies have expressed that if the definitions in the proposed rule were more aligned with those relating to privacy laws, around which compliance programs have already been built, they would be in a better position to comply. In that regard, some of ITI's companies believe that widespread identifiers like device identifiers or IP addresses should be exempt unless they would render U.S. persons identifiable to transacting counterparts.

Regarding the CISA security requirements, DOJ asked if companies are not already using many of these requirements to secure their data and whether these rules would necessitate companies now having to implement new measures to do so. ITI stated that while companies are already securing data, the CISA requirements have flexibility in certain requirements. ITI is concerned with system-level requirements (such as the requirement to patch vulnerabilities in a certain time frame), which seem inflexible. Given the variety of systems implicated, ITI believes this will cause challenges in compliance.

ITI expressed that companies seek more clarification on how DOJ and CISA's requirements work in tandem with one another and whether it was intention to include encrypted, anonymized, or de-identified data in the scope of the rule while then allowing those types security measures to be used to allow restricted transactions to go forward. DOJ stated that this was intentional By scoping in encrypted, anonymized, and de-identified data, we can ensure that we build in

baseline security for bulk sensitive personal data that is part of a restricted transaction while also ensuring that restricted transactions aren't impeded.

Additionally, ITI raised concern that the thresholds in the proposed rule are low. They noted that the values are the middle of the ANPRM ranges. DOJ asked ITI if the concern was more so on the ranges set just for CPI and geolocation data given the ubiquity of that data. DOJ also asked if the thresholds are essentially de minimis and almost any company with sensitive personal data that conducts business with a country of concern or covered person would need to comply with the rules. ITI reiterated the ubiquity of CPI and precise geolocation data, but noted they see concern with all of the thresholds. In response to Commerce, ITI also stated that they would not be proposing any specific threshold values, including in their NPRM docket comment. They cited the difficulties present in determining an exact number, noting that the thresholds would capture most businesses unless they were higher.

ITI asked DOJ if it would be helpful to copy CISA on their NPRM comment. DOJ replied that this is not necessary as DOJ is also checking CISA's docket for comments applicable to DOJ.

ITI asked DOJ for the timeline of the final rule's publication, to which DOJ replied that it will likely be published in January 2025. It will be a final rule as opposed to an interim final rule.

ITI had no further questions.