Federal Register Notice 87 FR 35250, https://www.federalregister.gov/documents/2022/06/09/2022-12432/request-for-information-on-advancing-privacy-enhancing-technologies, June 9, 2022

Request for Information (RFI) on Advancing Privacy Enhancing Technologies

Juniper Networks

July 8, 2022

Ms. Jeri Hessman
Technical Coordinator
NITRD
White House Office of Science and Technology Policy
490 L'Enfant Plaza SW
Washington, DC 20024

Re: Request for Information on Privacy-Enhancing Technologies (Docket 2022-12432)

Dear Ms. Hessman:

Juniper Networks submits these comments in response to the above-captioned Request for Information (RFI) regarding Privacy-Enhancing Technologies (PET). As a company dedicated to the security of networks, we appreciate NITRD's effort to develop a national strategy on privacy-preserving data sharing and analytics as well as associated policy initiatives. This submission provides background and recommendations in terms of networking technologies that can help ensure and enhance the privacy of data.

By way of background, Juniper Networks is a publicly-traded corporation headquartered in Sunnyvale, California. We develop high-performance networking solutions spanning routing, switching, security, wireless, and network management. Juniper Networks is a proud provider to the US government, major enterprises, cloud providers, and service providers around the world.

While Juniper does not collect personally-identifiable information as part of its business model, our customers rely on our solutions to transmit and protect their own data – personal, business confidential, and otherwise – that is critical to their operations, their employees,

and their own customers. The nature of our business and solutions leads our submission to address a particular issue that the RFI raises:

> Information about technical specifics of PETs that have implications for their development or adoption. This includes information about specific PET techniques that are promising, recent or anticipated advances in the theory and practice of PETs, constraints posed by limited data and computational resources, limitations posed by current approaches to de-identification and deanonymization techniques, limitations or tradeoffs posed when considering PETs as well as technical approaches to equity considerations such as fairness-aware machine learning, security considerations based on relevant advances in cryptography or computing architecture, and new or emerging privacy-enhancing techniques. This also includes technical specifications that could improve the benefits or privacy protections, or reduce the risks or costs of adopting PETs.

This paragraph of the RFI is critical because cybersecurity, cryptography, and computing architecture are key to maintaining privacy when sharing data over a network. In fact, these are primary factors in our product development cycle.

There are several security-related advances in networking technology that serve to enhance privacy:

- Encrypted Traffic Analysis: Any data being transmitted through a network needs to be analyzed for malware and other threats. Many such threat detection and analytical tools on the market today require the decryption of data, which ultimately can lead to a loss of privacy or may not even be feasible. Providers of networking solutions, including Juniper, have solutions available today that can effectively analyze network traffic without decrypting it. This means network operators and owners can often detect threats hidden in encrypted traffic without intercepting and decrypting it, thereby enhancing privacy.
- Cloud-Based Threat Protection: Cloud-based solutions currently on the market allow operators to monitor their traffic for patterns against known command and control/beaconing profiles. These protection offerings delivery three functionalities: (1) Identify and display information about scanned files and communication patterns whether clean or infected and identify communication identifiers that improve the threat intelligence networks many systems are tied to today (IP details, ports, C2, etc.); (2) create and view allowlists and blocklists that list safe or harmful network nodes, and profiles that define what file types to submit for investigation; and (3) view various reports, such as most infected file types, top malwares identified, and

infected hosts. Because this is a web-based service, customers can provision it on an as-needed basis.

- Security Director and Security Incident and Event Management (SIEM): These provide cloud-based policy orchestration as well as threat detection and mitigation across organizations including automation actions that enable scale and playbook execution permitting non-expert practitioners to act on advanced threat mitigation. This enables organizations to protect data privacy across devices, users, and networks.
- Secure Access Service Edge (SASE) and Zero Trust Data Center: Organizations can extend and adjust their network security beyond traditional firewalls and enable remote employees to work in a secure manner and protect their personal information from cyber threats. Provisioning a consistent security policy model that behaves and enforces efficacy to the highest levels achievable was previously difficult or impossible in the security industry, but recent innovations have changed that paradigm and these advances enable organizations to realize these benefits throughout their entire environment.

Juniper believes that OSTP/NITRD policy should recommend that technologies such as these that detect and address cyber threats while protecting and enhancing privacy. End users are able to deploy these as needed in a variety of environments – including if the data in question is financial, medical-related, or mission critical.

Thank you for your consideration of these recommendations.

Sincerely,

Mike Spanbauer
Field CTO Security Architecture