ENCRYPTION POLICY, DECRYPTED

KEY POLICY ISSUES FOR LAWMAKERS

June 5, 2018 - Capital Visitor's Center

The National Security Institute and the R Street Institute hosted a panel discussion, Encryption Policy, Decrypted: Key Policy Issues for Lawmakers, which examined the technical and policy issues surrounding the encryption debate. The diverse panel of experts included Bryson Bort, Heather West, Robyn Greene, and Darren Dick. Paul Rosenzweig served as moderator.

DISCUSSION WRAP UP

The Technical Issues. Mr. Bort began his remarks by discussing the history of encryption including the use of the Clipper chip, the role of Cellebrite in the San Bernardino case, and the idea of having a key escrow, an arrangement in which the keys needed to decrypt encrypted data are held in escrow, and under certain circumstances, an authorized third party may gain access to those keys. Ms. West and Mr. Bort discussed the notion that technology companies currently have back door access through their system update processes but argued that a key escrow system is sufficiently different to represent significant risk to the systems. Mr. Bort noted that implementation of a key escrow system raises additional questions, such as who would build, maintain, or pay for such a system. Ms. West came out strongly against the government managing a key escrow system; she went on to say that because there is no such thing as uncrackable software, any key vault could ultimately be hacked.

The Policy Debate. Ms. Greene and Mr. Dick presented the policy positions for privacy and government access advocates, respectively, and discussed the government's ability to search and seize evidence in light of Fourth Amendment protections. Ms. Greene stated that while a warrant allows the government an opportunity to retrieve physical evidence, such as a phone, a warrant does not include granting law enforcement the technological means to unlock an encrypted phone.

SPEAKERS

BRYSON BORT
Founder & CEO, SCYTHE

Darren Dick
Director of Programs, National Security Institute

Robyn Greene
Policy Counsel and Government Affairs Lead, Open Technology Institute, New America

Heather West
Senior Policy Manager, Americas Principal, Mozilla

Moderator:
Paul Rosenzweig
Senior Fellow,
R Street Institute
Advisory Board Member,
National Security Institute

The Policy Debate Continued. Mr. Dick argued that in crafting the Fourth Amendment, the framers clearly intended that the government have the opportunity to seize the information sought where the government could meet the Amendment's probable cause and reasonableness standards. Mr. Dick also noted that a number of technology companies that argue for absolute privacy vis-à-vis the U.S. government are often willing to turn over customer information to other governments with lower individual privacy protections, such as China.

Ms. Greene stated that as users increasingly use their phones as authenticators for logging into secure locations and resources, companies must make phones more secure in case of theft. Ms. Greene cited data showing that increased encryption on the iPhone has yielded a sharp decline in phone thefts. She went on to say that requiring the tech companies to allow back door access of encrypted data to law enforcement actors could cause a chill on industry and potential unintended consequences.

Advancing the Debate. Although there is still much rancor in the debate, the panel agreed that the country is in a better place to push forward the conversation. Mr. Dick pointed out, however, that it would be impossible to move the conversation forward if both sides continued to view the issue as black and white. Rather, he suggested we view privacy as a spectrum and that more thought should be given to solutions between the two ends. Mr. Bort warned that the tech industry already harbors some mistrust in regards to government action but he and Ms. Greene reiterated that the industry understands that all parties must come to the table as any proposed solution requires buy in from all stakeholders.