wiley

PRESS RELEASE

Megan Brown Co-Authors National Security Institute's New Law and Policy Paper on 'Techlash and National Security: The Need for U.S. Leadership on Privacy and Security'

July 29, 2020

Washington, DC – Megan L. Brown, partner in Wiley's National Security, Privacy, Cyber & Data Governance, and Telecom, Media, & Technology practices, co-authored "Techlash and National Security: The Need for U.S. Leadership on Privacy and Security," a new law and policy paper published today by the National Security Institute (NSI) at George Mason University's Antonin Scalia Law School. The publication's announcement coincided with today's congressional hearings on major online platform players, and with the launch of NSI's Technology, Innovation, and American National Security program. NSI Senior Fellow Dr. Andrea Little Limbago, who is Vice President of Research and Analysis at Interos, serves as co-author on the paper.

"As policymakers consider tech policy, from privacy to cyber to encryption, they should resist a populist temptation to punish or regulate tech companies in a way that makes the U.S. less open to innovation, creativity, and investment," said Ms. Brown. "As we see in recent congressional and Executive branch actions, including today's antitrust hearing and yesterday's National Telecommunications and Information Administration petition to the Federal Communications Commission to revise Section 230, some are targeting our own tech sector while other countries promote national champions to promote their ideas around the world."

Related Professionals

Megan L. Brown
Partner
202.719.7579
mbrown@wiley.law

Practice Areas

National Security
Privacy, Cyber & Data Governance
Telecom, Media & Technology

"We need thoughtful policies that tackle our very real security and privacy challenges in order to promote innovation and lead on the global stage," Ms. Brown added. "The United States must be an active counterweight to geopolitical rivals. And it must so do in a way that keeps the U.S. private sector engaged and empowered to take a leading role in global technology markets."

"Data is foundational to our national and economic security, and is at risk of manipulation, theft, and exposure from a broad range of state and non-state actors," said co-author Dr. Limbago. "The ongoing revelations of data-sharing scandals by tech companies has prompted growing interest in new data regulations. Given the foundational role of data to our national and economic security, this is a welcome shift, but risks weakening instead of strengthening national security and data protection."

"This paper highlights the essential role the U.S. must play in shaping a data protection strategy that supports both privacy and security, and provide the leadership to demonstrate how innovation and data protection can co-exist as a foundational component of a digital democracy," Dr. Limbago added.

The paper has direct relevance to today's hearing because it:

- Summarizes how "Techlash" (defined as the "strong and widespread negative reaction to the growing power and influence that large technology companies hold") and criticism of Big Tech are realigning the regulatory instincts of policymakers and companies. This dynamic may embolden government action to regulate in the name of lawful government access and national security, among other goals.
- Describes how movements to regulate technology companies may undermine privacy and security protective end-to-end encryption and erode Section 230 of the Communications Decency Act.
- Suggests that policymakers should prioritize data protection as essential for national security in the digital era, and urges U.S. global leadership to inspire digital democracies and counter digital authoritarianism.
- Proposes actionable recommendations for policymakers to address encryption, federal data protection regulation, cybersecurity expertise, and global leadership.

The paper is available here. NSI's news release on the paper can be found here.

Ms. Brown – who served in the U.S. Department of Justice as Counsel to two U.S. Attorneys General – is a Senior Fellow and Program Director for NSI's Cybersecurity Law & Policy Program. She regularly speaks and writes on security and privacy, and previously published Privacy Regulation and Unintended Consequences for Security and Cyber Imperative: Preserve and Strengthen Public-Private Partnerships for NSI. Additionally, she is co-author of a pivotal IoT Security Report published by the U.S. Chamber of Commerce.

Ms. Brown serves on the U.S. Chamber's Cybersecurity Leadership Council and is on the Board of the Women's High-Tech Coalition (WHTC). In her WHTC role, she helped launch earlier this year the "Tech Talks Pandemic" podcast series, where policymakers and private-sector practitioners discuss the ways in which technology is helping to address the pandemic.

Wiley has an unparalleled ability to assist clients on a broad range of national security issues. The firm's Privacy, Cyber & Data Governance Practice provides clients with a thorough understanding of the current and potential obligations and risks that are associated with privacy, data security, and cybersecurity, along with a comprehensive range of compliance and strategic advice, from advice for Boards and senior management to managing government investigations into security incidents. Wiley covers emerging technology and security trends at our blog, WileyConnect.com, where we also host regular podcasts on technology law and policy, including cybersecurity.