MAYER | BROWN

Over the Horizon:

Cybersecurity & Data Privacy Policy in the Next Administration

Matthew J. Eggers
Vice President, Cybersecurity Policy
US Chamber of Commerce

Tommy Ross
Senior Director
Business Software Alliance

Stephen Lilley
Partner
Mayer Brown LLP

Denise E. Zheng
Vice President
Business Roundtable

October 28, 2020

Speakers

Matthew J. Eggers

Vice President, Cybersecurity Policy

US Chamber of Commerce

Tommy Ross

Senior Director

Business Software Alliance

Denise E. Zheng

Vice President

Business Roundtable

Today's moderator:

Stephen Lilley

Partner

Mayer Brown LLP

Introduction

- 2020 saw major developments in cybersecurity and data privacy policy, including:
  - Debates over national data privacy increasing as the COVID 19 pandemic created new challenges and amendments to the CCPA were put on the ballot;
  - The Court of Justice of the European Union invalidating the Privacy Shield;
  - The Cyber Solarium issuing its report and recommendations; and
  - Regulators across sectors focusing on cybersecurity and data privacy.
- Cybersecurity and data privacy issues are likely to continue to be a focus for policymakers in 2021, regardless of who wins the upcoming presidential election.
- Today we will discuss priority cybersecurity and data privacy policy issues as we head into the election—and what companies should watch for next year.

Agenda

- National data privacy legislation
- Data transfers after *Schrems II*
- The Internet of Things
- Critical infrastructure
- Supply chain
- Government contracting
- Cyber norms and cyber conflict
- Structure of U.S. government cyber leadership

National Data Privacy Legislation

- Privacy laws continue to change on the state level.
  - CRPA is on the ballot in California and other states are considering CCPA-like legislation.
  - State data breach statutes continue to evolve.
- Calls for federal data privacy legislation have continued to grow, particularly in light of the challenges posed by the COVID-19 pandemic and questions raised by new technologies.
- Significant consideration has been given to national data privacy legislation in Congress. For example, on September 17, 2020, Chairman Roger Wicker of the Senate Commerce Committee, along with Senators Thune, Fischer, and Blackburn, introduced the SAFE DATA Act, S. 4626, which would create various new privacy rights and compliance obligations, with enforcement by the Federal Trade Commission.

Data transfers after *Schrems II*

- On July 16, 2020, the Court of Justice of the European Union delivered its long awaited decision on the validity of the European Commission's Standard Contractual Clauses and the EU-US Privacy Shield.
  - The CJEU invalidated the Privacy Shield for transfers to the United States.
  - The CJEU concluded that businesses can continue to rely on Standard Contractual Clauses for transferring personal data from the EEA provided that the level of protection of the transferred data is adequate.
- The Department of Commerce has sought to provide certainty for U.S. businesses, including through the September release of a white paper on U.S. privacy protections.

The Internet of Things

- Federal procurement may play a very significant role in IoT cybersecurity going forward. The IoT Cybersecurity Improvement Act passed the House of Representatives in September 2020. The bill would require NIST to create cybersecurity standards for IoT devices purchased by the federal government and would task OMB with promulgating implementation guidance.
  - The legislation also would address coordinated disclosure and vulnerability management in IoT devices purchased by the federal government.
  - Similar legislation passed out of committee in the Senate in 2019.
- Regulatory scrutiny of IoT device security and privacy also has continued.

Critical infrastructure cybersecurity

Critical infrastructure cybersecurity continues to be a focus area for policy makers. For example:

- FERC began an inquiry into whether CIP Standards adequately address data security; anomaly detection; and cyber event mitigation.
- Congress reauthorized the CFATS program for three years.
- Legislation authorizing DHS to subpoena ISPs to identify vulnerable critical infrastructure systems has been included in drafts of the 2021 NDAA.
- The Department of Energy announced a new vulnerability testing collaboration through its CyTRICS program.
- DHS' Cybersecurity and Infrastructure Security Agency issued a new five-year strategy for securing industrial control systems.

Supply chain

- Supply chain security has been a priority issue for the Trump Administration. Action has been taken through executive orders and related regulatory action.
  - 2020 Executive Order on Securing the United States Bulk-Power System;
  - 2019 Executive Order on Securing the Information and Communications Technology and Services Supply Chain.
- NTIA continues to lead collaboration on Software Bill of Materials (SBOMs).
- NTIA announced the establishment of the Communications Supply Chain Risk Information Partnership (C-SCRIP).
- NIST has weighed in on "Mitigating the Risk of Software Vulnerabilities by Adopting a Secure Software Development Framework."

Government contracting

- Section 889 of the National Defense Authorization Act for 2019 prohibited the procurement of products or services incorporating certain Chinese technology or their use by contractors.
  - Part A of Section 889 generally prohibited the procurement of the covered products by the U.S. Government.
  - Part B of Section 889 generally prohibited the use of the covered products by U.S. contractors.
  - Rulemaking to implement Section 889 continued into 2020.
- The Department of Defense also issued Version 1.02 of the Cybersecurity Maturity Model Certification in March 2020.

Cyber norms and cyber conflict

- The Cyber Solarium identified "strengthen[ing] norms and non-military tools" as a pillar of its strategy of layered cyber deterrence. Its recommendations included:
  - Creating a new Assistant Secretary of State position with responsibility for cybersecurity;
  - The executive branch engaging actively and effectively in forums setting international information and communications technology standards;
  - Improving international tools for law enforcement activities in cyberspace.
- In a recent speech, the Assistant Secretary of State for the Bureau of International Security and Nonproliferation confirmed that the government is not pursuing "Arms Control" in cyberspace, but is pursuing both frameworks for responsibility and restraint, as well as cyber deterrence.

Structure of U.S. government cyber leadership

- The Trump Administration eliminated the "Cyber Czar" position within the White House in 2018.
  - The Trump Administration stated that the move would help streamline management within the National Security Council.
  - Numerous policy makers questioned this decision, raising concerns about a loss of coordination on cyber policy within the White House and across the Administration.
- The Trump Administration has built up the Cybersecurity and Infrastructure Security Agency within DHS, which was created by Congress in the CISA Act of 2018.
- The organization of cyber leadership within the State Department has also been a matter of significant debate, including with respect to the creation of a new cyber bureau led by an Ambassador-at-large.

Americas | Asia | Europe | Middle East

mayerbrown.com