The Biden Approach to Privacy and Cybersecurity

ROPES & GRAY

May 13, 2021

AGENDA

- Cyber Threats from Foreign Nation States
- The Role of Federal Agencies
- Trends in State Privacy Laws & Likelihood of Federal Privacy Legislation
- Role of the Courts
- Negotiation of a New Data Protection Equivalence Agreement following *Schrems II*
- Questions

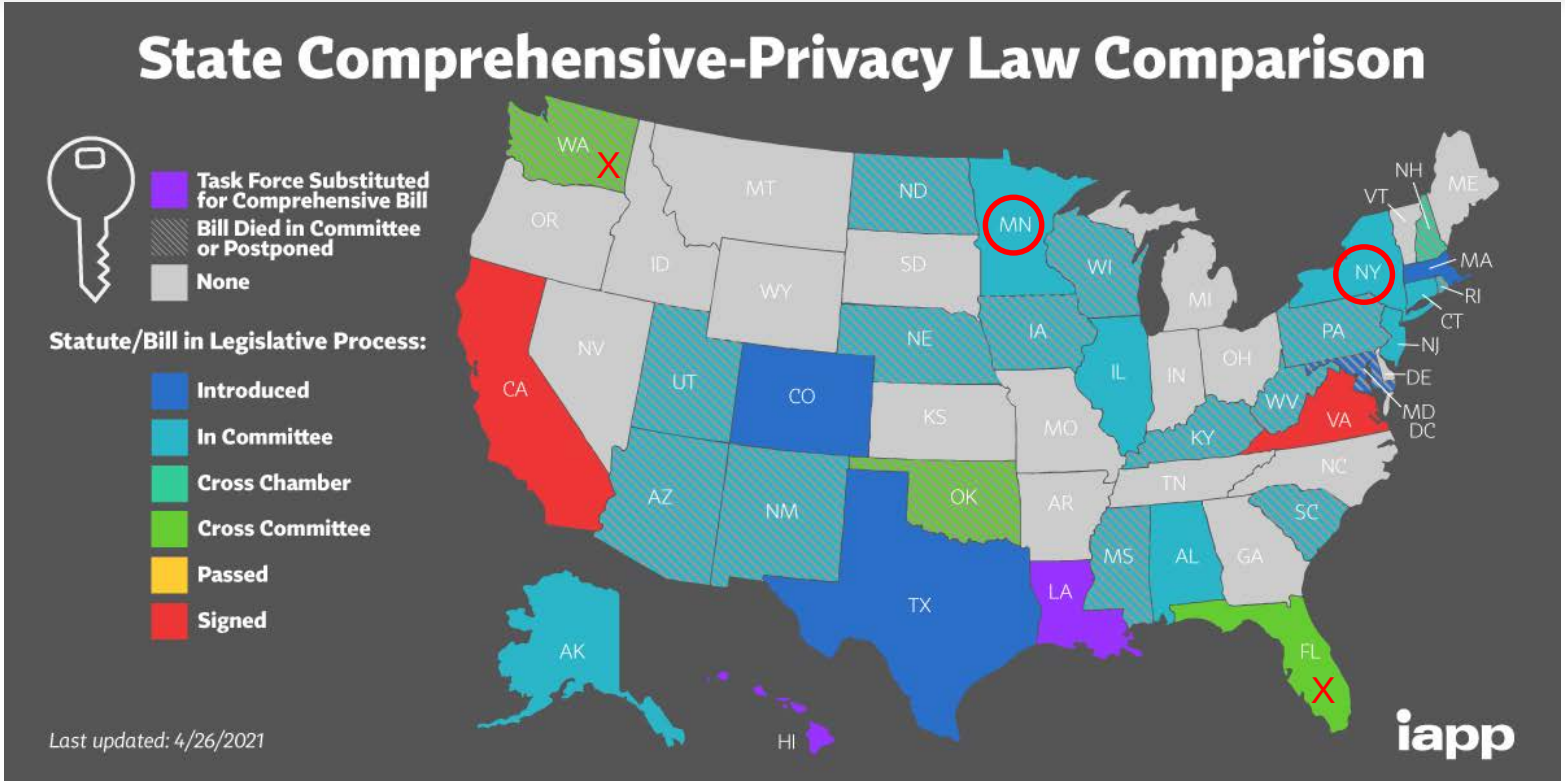
Cyber Threats from Foreign Nation States

- We have seen extensive attacks from Russia and China against several pieces of the U.S. technology infrastructure
- How can the U.S. defend against these attacks while simultaneously preserving privacy and civil liberties?
- U.S. companies need to feel comfortable working with other U.S. companies and working globally without the threat of a cybersecurity attack from foreign nation states.
- Recommendations of the Cybersecurity Solarium Commission
  - Leading document on cybersecurity strategy in the United States currently
  - Emphasizes importance of defending forward
- Robust cooperation between the private and public sectors is needed
- ISACs and ISAOs need to be able to share information without the fear of violating privilege or raising antitrust issues
- Organizing that effort will be the key challenge of the Biden administration for cybersecurity

Roles of Federal Agencies

- The **Federal Trade Commission** is expected to be a leading player
  - New Chair
  - Recent Enforcement Actions
  - Data Stewardship Model
- The **SEC** and their Office of Compliance Inspections and Examinations (OCIE) continue to publish guidance and exam observations
- **NIST**: Released Jan. 16, 2020, currently focused on governmental privacy, the NIST cybersecurity framework has become mandatory for government contractors and influential in the private sector
- **OCR Settlements**: HHS OCR continues to pursue enforcement actions against healthcare providers who allegedly violate patients' HIPAA mandated right of access to health records
- Recent **OFAC** Ransomware Payment Advisory
- Recent **OMB** guidance for federal agencies concerning the use of AI.

Other State Developments



State Developments: California

- **CCPA Implementation and Regulations**: Final regulations filed August 14, 2020 address key areas, including record-keeping and requirements for responding to consumer requests, and have caused significant upset for behavioral advertising industry
- **CPRA Passed in November**: new provisions generally enter into force Jan. 2023
  - Requires businesses to engage in data minimization, disclose retention periods for each category of personal information, communicate deletion request to third parties to whom the business has sold or shared personal information, and to contractually bind third parties to cooperate with data subject requests.
  - Establishes a new California Privacy Protection Agency
  - Creates a new category of Sensitive Personal Information (SPI)
  - New rights, including right to opt out of *sharing* of personal information
  - Damages available for exposure of email and password

State Developments: Virginia

Virginia Consumer Data Protection Act (CDPA): will come into effect January 1, 2023 simultaneously with California's Consumer Privacy Rights Act (CPRA).

- Gives VA consumers rights to access, correct, delete and obtain a copy of personal data and to opt out of certain data processing activities.
- Applies to personal data about consumers (acting as consumers, not employees or B2B)
- Applies to businesses that target Virginians and meet threshold of personal data processing
  - Exemptions: GLBA, HIPAA, certain government entities, non-profits, and higher education institutions, as well as information subject to certain federal laws
- Personal data is anything linked to an individual
  - Exemptions: publicly identifiable, de-identified, data tied to household but not individual
- Borrows from GDPR: Controllers/Processors, Data Protection Assessments, Consent, Sensitive Data
- Enforcement solely by the State AG, with no private right of action

State Developments: New York

- **Stop Hacks and Improve Electronic Data Security Act (SHIELD Act):** effective as of October 23, 2019, and broadened NY's data breach notification statute (NY Gen. Bus. L. §899)
- **NYDFS Enforcement Action**: On July 22, 2020, NYDFS filed its first cybersecurity enforcement action against First American Title Insurance Company seeking civil monetary penalties for six violations of the cybersecurity regulation
  - Alleges First American exposed hundreds of millions of documents containing NPI as a result of vulnerabilities, deficient controls, and other flaws in cybersecurity practices
  - Illustrates importance of maintaining information security policies, establishing internal security controls, and appropriately assessing and categorizing risks
- **New York Privacy Act**: Proposed legislation goes farther than CCPA and creates "data fiduciary" concept
  - Entities collecting and controlling data would owe fiduciary duties to protect individuals' personal data, a breach of which could give rise to tort claims

State Developments: Massachusetts

- **In August, Massachusetts AG Maura Healey announced new Data Privacy and Security Division within her office** to "protect consumers from the surge of threats to the privacy and security of their data in an ever-changing digital economy."
- Sara Cable, Director of Data Privacy and Security within the OAG's Consumer Protection Division, promoted to Chief of new Division
- Stated purpose to:
  - Empower consumers in the digital economy
  - Ensure that companies are protecting consumers' personal data from breach
  - Protect equal and open access to the internet
  - Protect consumers from data-driven technologies that unlawfully deny them fair access to socioeconomic opportunities

Other State Developments

- Nevada passed a law in 2019 that was similar to, but less extensive than, CCPA. Amendments are pending.
- Washington and Florida recently failed to pass similar bills before the end of their respective legislative sessions, due to disagreements over the private right of action.
- Minnesota, Oklahoma, Connecticut, and Illinois all have bills pending that resemble CCPA/CDPA.
- Following Illinois and New York, Maryland recently introduced a biometric information privacy bill.
- Possibility of federal legislation?

The Courts

- Tension between the First Amendment and Purpose Limitations in privacy laws
- Shifting court interpretations of the Computer Fraud and Abuse Act (CFAA)
- Courts' role in refining the Telephone Consumer Protection Act (TCPA)

New Data Protection Equivalence Agreement Following *Schrems II*

- EU-US Privacy Shield was put in place to bridge equivalency gap for American businesses to transfer personal data outside of the EEA
- Recent *Schrems II* decision invalidated the EU-US Privacy Shield
- U.S. White Paper:
  - Sets out three key principles in assessment of the U.S. legal position regarding EU-U.S. Data Transfers, and articulates U.S. Government view that three statutes would provide ability for any aggrieved person, from any country, to challenge surveillance under a FISA § 702 order
  - But causes of action under these statutes are complex; challengers to surveillance would face limitations
  - European Data Protection Board (EDPB), adopted "Recommendations on the European Essential Guarantees for Surveillance Measures" to assist with the evaluation of third-country surveillance laws
- EDPB guidance on transferring data without the Privacy Shield says to supplement the Standard Contractual Clauses (SCCs) with other protections such as encryption or increased transparency
- Waiting for revised SCCs (drafts have been published) and for a replacement for the Privacy Shield
- Predictions vary, but revised SCCs will almost certainly arrive sooner than a replacement Privacy Shield

Questions?