RSAConference2020

San Francisco | February 24 – 28 | Moscone Center

HUMAN ELEMENT

SESSION ID: LAW-T08

Hot Topics in Cyber-Law 2020

MODERATOR: **Michael Aisenberg**
Principal Cyber Policy Counsel
The MITRE Corporation

AMERICAN BAR ASSOCIATION
Science & Technology Law Section

PANELISTS: **Catherine Barrett**
Cyber Policy Principal
The MITRE Corporation

Lucy Thomson
Attorney
Livingston PLC

Stephen Wu
Shareholder
Silicon Valley Law Group

RSAConference2020

AGENDA

- …And Now the News: Selected Key 2019-20 Policy Developments
- Hot Topics
  - Data
  - Election Technologies
  - California—and Artificial Intelligence

ABA AMERICANBARASSOCIATION
Science & Technology Law Section

RSAConference2020

..AND NOW THE NEWS HEADLINES FROM D.C.:

National Defense Authorization Act for 2020

- Series of significant ICT and Supply Chain policy measures, applicable to DoD, & WoG

- ***Open Government Data Act of 2019* ('OGDA')**
  - **"possibly the most important govt. information legislation since FOIA"…changing the way we use data**
  - ***Open Government Data Act*, Title II of Foundation for Evidence-based Policymaking Act of 2018, Public Law 115-411, signed 14 January 2019.**
- ***California IOT -Connected Devices Security Act***
  - **Adds Title 1.81.26 (Sec. 1798.91.04) to Part 4 of Div. 3 of the CA Civil Code *unlike CCPA, focus on vendor obligation, rather than citizen remedy after abuse of data!)***

- **S. 3045 @CISA Director Makes Case for Subpoena Power over Internet Service Providers (Christopher Krebs, Director of DHS's Cybersecurity and Infrastructure Security Agency, testified in support of the S. 3045 *Cybersecurity Vulnerability Identification and Notification Act***

RSAConference2020

EO 13859 Maintaining American Leadership in Artificial Intelligence, February 11, 2019 …84 Fed.Reg. 3697. –One year ago !

EO 13873: Securing the Information and Communications Technology and Services Supply Chain May 15, 2019 …84 FedReg 22689

NIST SP 800-161 *Draft revision of Supply Chain Risk Management guidance document* RFC just released Feb 5, 2020

2019 FBI Internet Crime Report
(FBI News Blog) Feb 11, 2020

@NIST seeks comment on *updates to National Vulnerability Database*
(Inside Cybersecurity, Feb 12, 2020

RSAConference2020

DATA!

Catherine Barrett JD, SSCP
Cyber Policy, Principal
MITRE Corp.
cabarrett@mitre.org

DISCLAIMER:

The speaker's affiliation with The MITRE Corporation is provided for identification purposes only and is not intended to convey or imply MITRE's concurrence with, or support for, the positions, opinions, or viewpoints expressed by the speaker.

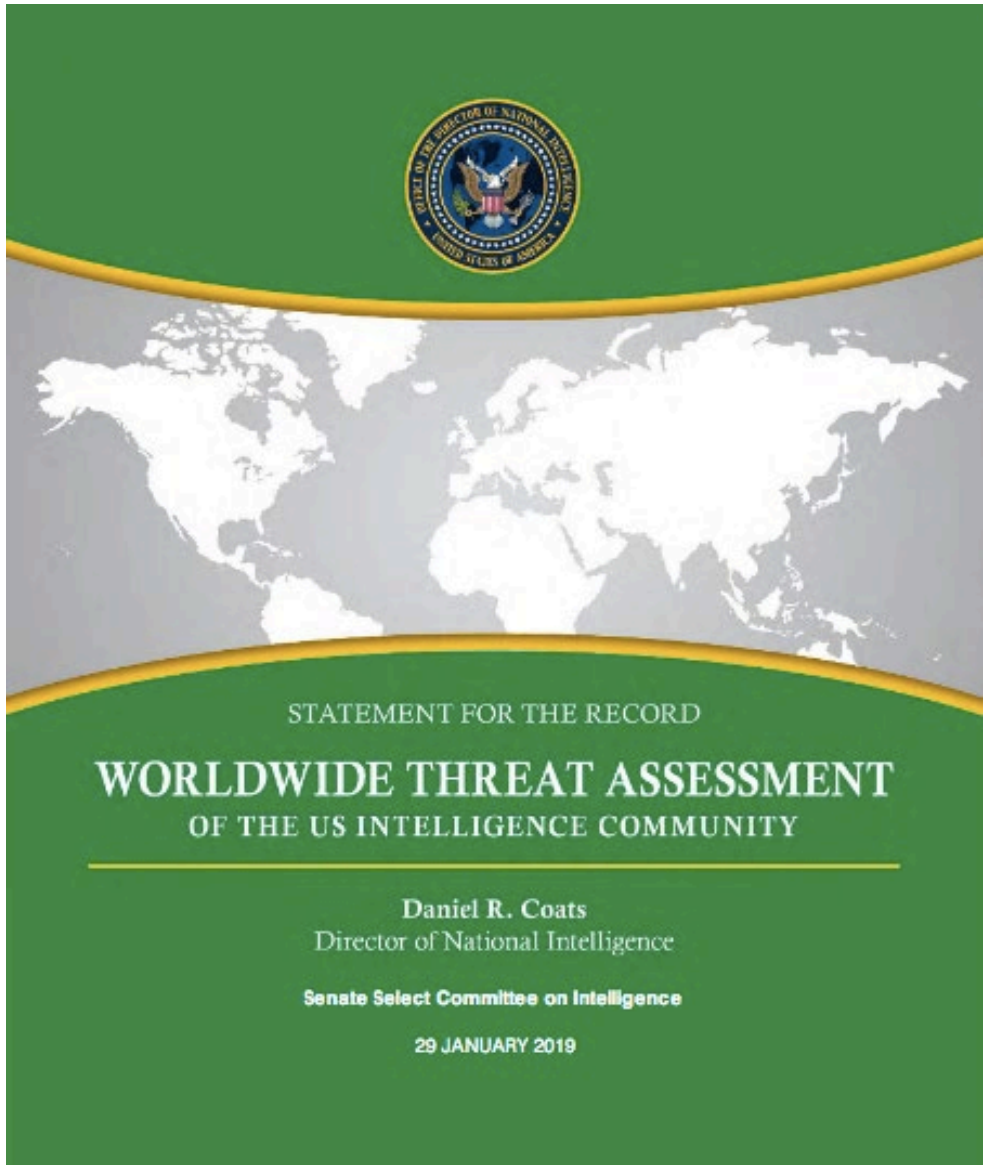
Analysis of data broker laws (pending legislation appears in gray)	CA	VT	IL	MA	WA
Data protections apply to an individual or natural person residing in the state (consumers)	✓	✓	✓	✓	✓
Data brokers are business that knowingly sell or license consumer data to third parties; Do not have a direct relationship with consumers	✓	✓	✓		✓
Data brokers required to register with the state	✓	✓	✓		
Data broker registry is public	✓	✓			
Data broker duty to protect personally identifiable information (PII)	✓	✓	✓		
Data brokers face penalties for failure to register (civil fines, fees, injunction)	✓	✓	✓		
Data broker must provide administrative, technical and physical safeguards as part of an information security program	✓	✓	✓		
Consumer private right of action against data broker		✓	✓		

RSAConference2020

Hacking Democracy

Lucy L. Thomson, Esq. CISSP, CIPP/US

February 2020



THE THREAT LANDSCAPE

The potential for surprise in the cyber realm will increase in the next year and beyond as billions more digital devices are connected – with relatively little built-in security – and both **nation states and malign actors become more emboldened and better equipped** in the use of increasingly widespread cyber toolkits. . . .”

Our adversaries and strategic competitors probably already are **looking to the 2020 US elections** as an opportunity to advance their interests. More broadly, US adversaries and strategic competitors almost certainly will **use online influence operations** to try to weaken democratic institutions, undermine US alliances and partnerships, and shape policy outcomes in the United States and elsewhere.

Adversaries and strategic competitors also may seek to **use cyber means to directly manipulate or disrupt election systems**—such as by tampering with voter registration or disrupting the vote tallying process—either to alter data or to call into question our voting process.

THE COMPLEX ELECTON ECOSYSTEM – STAKEHOLDERS/ POTENTIAL ATTACK SURFACES

9,000 U.S. jurisdictions administer elections, ~ 175,000 precincts

LAWS, POLICIES, PROCEDURES, & STANDARDS

Policy-makers

Federal
- Congress
- DHS and EAC

State
- Secretaries of State
- State legislatures

Local
- Election officials

Private
- Election system manufacturers
- 3P technology contractors

CANDIDATES & CAMPAIGNS

Candidates

- Candidate filing system/ Qualifications

Campaigning

Debates

Media & Messaging

Social Media
- Platforms
- Monitoring (Facebook, Twitter)
- "Fake News"

VOTING – *Voters*

- Voter information system

Voter Registration
- Local/ DMV/ post office
- Online

- Voter registration database
- Voter authentication system
- Electronic pollbooks

VOTING (early, absentee, and election day)

1) Onsite
- e-Pollbooks/ barcode scanner
- Paper ballots
- DREs
- Optical scanners

2) Mail (OR, WA, CO + 19)
- Ballot delivery/return

3) Internet (30 states)

ELECTION ADMINISTRATION

Election Officials

(re)Districting

Ballot questions
- ERIC – voter registration verification/ state information sharing

Election Management Systems

Third Party Tech Contractors
- Ballot creation system
- Voting equipment configuration
- Ballot Tracking system (printing/ delivery/ return)
- Central tabulators/ vote tallying
- Election night reporting (ENR) – statewide/unofficial
- Certify: final election results
  - Canvass
  - Audits
  - Recounts

OUTSOURCING ELECTIONS
"Election Technology Industry"

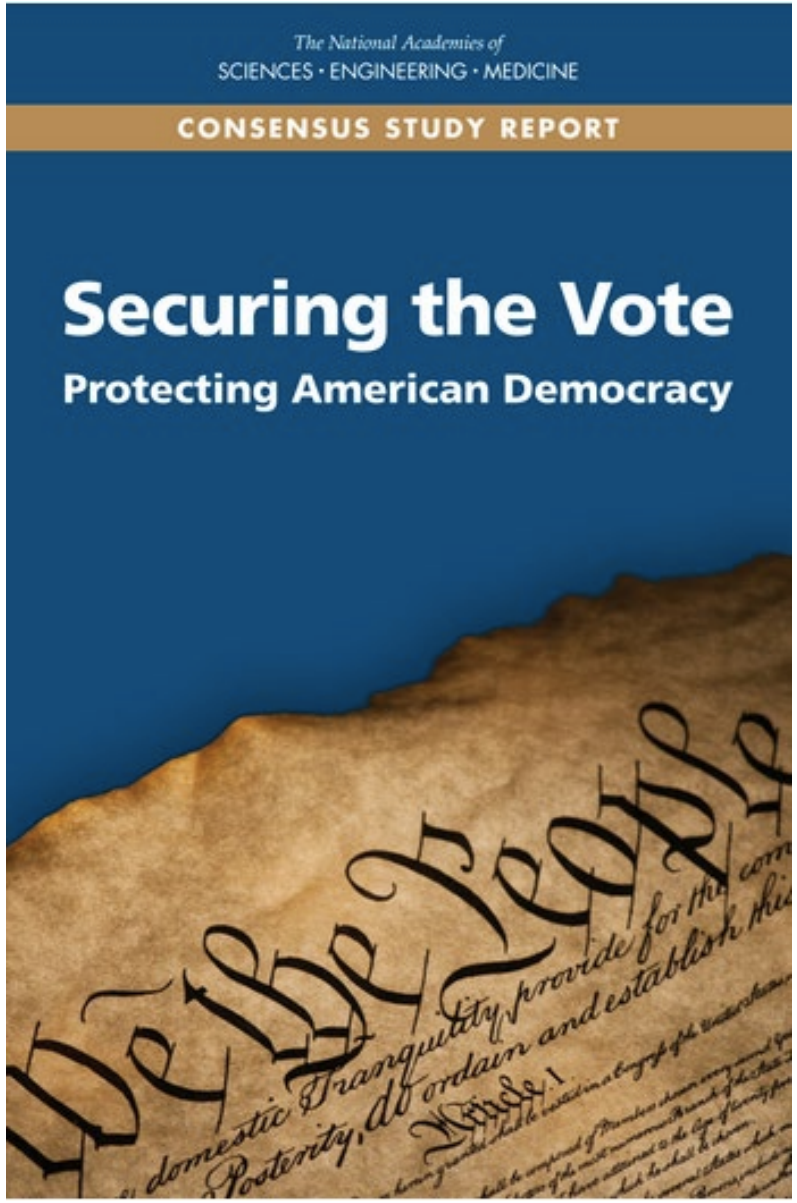
- **Three top-tier vendors cover 92 percent of total eligible voters**

- **Six other firms provide specialized technology**

- **Private sector's role in supporting elections**
  - Sell ***Integrated Voting Solutions*** to state and local election officials, typically including a package of hardware, software, services, and support
  - Manage ***Databases*** – *voter registration, e-pollbooks, candidates*
  - Manufacture ***Voting Machines***
    - Design ***Ballots***
    - Develop software to program machines
  - Host ***Results Websites***
- **Over 60 percent of American voters cast ballots on systems owned and operated by a single vendor**
  - Potential for a single point of failure
  - Exploitation point for hackers to target election systems
  - Supply chain risks
  - Ownership issues

CONSENSUS RECOMMENDATIONS

- To protect the integrity and security of U.S. elections, all local, state, and federal elections should be conducted using **human-readable paper ballots** by the 2020 presidential election.
- States should mandate a specific type of audit known as a **"risk-limiting" audit** prior to the certification of election results.
- **Internet voting should not be used** at the present time, and it should not be used in the future until and unless very robust guarantees of secrecy, security, and verifiability are developed and in place.
- Election administrators should routinely assess the **integrity of voter registration databases** and put in place systems that detect efforts to probe, tamper with, or interfere with voter registration systems.
- Jurisdictions that use **electronic pollbooks** should have **backup plans in place** to provide access to current voter registration lists in the event of any disruption.
- Election systems should continue to be considered as U.S. Department of Homeland Security-designated **critical infrastructure**.



KEY STEPS TO PROTECT ELECTION SYSTEMS

1) **Replace aging, outdated, vulnerable voting machines with voter-verified paper ballots**
2) **Conduct Post-election Audits –** check that voting systems properly counted ballots
3) **Adopt and Follow Cybersecurity Standards, Guidelines and Best Practices**
4) ***Funding* – Address Chronic Underfunding of Elections**

2020 Federal Grants to States for Election Security Improvements

- **Consolidated Appropriations Act**, 2020, Pubic Law 116-93 became law on 12/20/19
  - $425 million for the Election Assistance Commission (EAC) to make election security grants to states "for activities to improve the administration of elections for Federal office, including to enhance election technology and make election security improvements."
  - No cybersecurity *requirements;* NIST cybersecurity guidelines are voluntary
- **National Defense Authorization Act for FY 2020,** S. 1790, Public Law 116-92
  - Section LXV, Election Matters

RSAConference2020

CALIFORNIA: DATA, IOT, AI

Stephen Wu, Esq.
Silicon Valley Law Group
February 2020

California Consumer Privacy Act

- Road to CCPA, and old categories of personal info
- AB 375, approved June 28, 2018, effective 1/1/2020
- Civil Code 1798.100-1798.198
- Several amending laws signed in 2019
- Regulations proposed (plain language, request handling and verification, discrimination)
- Ballot initiative: California Privacy Rights and Enforcement Act (CPRA)

CCPA – Who is Covered?

- Larger businesses not already regulated by health or fin service laws)
- Business thresholds: $25 M in company revenue, PI on 50,000, or 50% or more revenue from the “sale” of PI.
- Who is protected? California “consumers”/residents (can be employees) while in Cal.
- Broader definition of “personal information” than before (11 categories)
- Non-discrimination right

CCPA Requirements

- Notice and transparency
- Data subject access requests (e.g., categories, actual data, erasure)
- Effect on workers in 2020
- Business-to-business transactions in 2020 (business card information)

CCPA Enforcement and Effect

- AG proposed regulations
- General privacy enforcement: AG action
- Not a basis for private right of action under other law (UCL)
- GDPR Lite?
- Federal legislation effect

Breach Liability in CCPA

- Private right of action for violations involving a breach (30-day cure period)
  - Only covers larger CCPA-covered businesses
  - Dollar amount per violation (statutory damages)
- $100-750 per incident statutory damages or actual damages
- Promotes enforcement of AB 1950 reasonable security for covered ”personal information”
- Effect on security practices and management

Artificial Intelligence

- Artificial intelligence data protection challenges
- Artificial intelligence as a data protection enabler
- New legislation and guidance

Apply: “Hot Topics” is NOT a Crystal Ball

- But we hope it is a useful tool, offering you detail you have not learned elsewhere, or understood unforeseen consequence.
- We seek to usefully extend your understanding of critical issues’ impact on your practice/business
- As with all law and policy knowledge, the value you derive from this depends on your unique situation (“IT DEPENDS!”)—but first, pay attention !
  - Be prepared to do additional research: we have not briefed cases for you
  - But, we ARE HAPPY TO ENGAGE, ANSWER QUESTIONS AND DIRECT YOU TO FURTHER RESOURCES, SO:
- ASK, FOLLOW UP, USE CITATIONS TO LEARN MORE !!
- COME TO OTHER LAW TRACK SESSIONS !!!

AMERICANBARASSOCIATION

Science & Technology Law Section

Future Programming

- American Bar Association Internet of Things National Institute, Washington, D.C., April 29-30, 2020, ambar.org/iot2020
- American Bar Association Artificial Intelligence and Robotics National Institute, Santa Clara, CA, October 12-13, 2020, ambar.org/ai2020

RSAConference2020

Thank You!

For more information:

Catherine Barrett: cbarrett@mitre.org
Lucy Thomson: lucythomson1@mindspring.com
Steve Wu: ssw@svlg.com
Michael Aisenberg: maisenberg@mitre.org