

Privacy Legal Update

MICHAEL HELLBUSCH, CIPP/US/E, CIPM
PARTNER, RUTAN & TUCKER

Updates and other considerations for
businesses amid the COVID-19
pandemic



Who we are
and what we do



Rutan & Tucker's practice extends nationwide, while maintaining our connection to the fabric of California. Rutan & Tucker continues to distinguish itself as one of California's largest full-service law firms, as it has for decades, with a significant presence in Orange County, Silicon Valley and San Francisco.

PRACTICE AREAS

Government
& Regulatory

Intellectual
Property

Corporate
and Tax

Privacy and
Security

Litigation &
Trial

Real Estate

Summary of Topics

- Updates to the CCPA Regulations
- Delayed Enforcement of the CCPA?
- Status of State and Federal Privacy Bills
- Privacy & Data Security During a Pandemic
- Contractual Obligations During a Pandemic
- Additional Resources

Main points covered

A black and white photograph of a desk. In the foreground, there is a white coffee cup filled with a frothy beverage, sitting on a matching saucer with a spoon. To the left, a laptop is partially visible, showing its keyboard. Several papers are scattered on the desk, some with text and diagrams. A smartphone is visible in the bottom left corner. The background is slightly blurred, showing more of the desk and some office supplies.

CCPA Regulations

Second Set of Modifications

The Attorney General's Office issued a 2nd Set of Modifications to Proposed CCPA regulations on March 11, 2020.

Comments to the modifications must be received by March 27th at 5 p.m.

Major Changes



Interpretation of the CCPA

Removed a section that provided guidance on what is "personal information" under the CCPA.

The "Do Not Sell My Info" Button

The proposed DNS button previously proposed has been deleted. Businesses must still provide a link if they sell personal information.

Privacy Policy Update

The privacy policy requires less granularity about data collection and use.

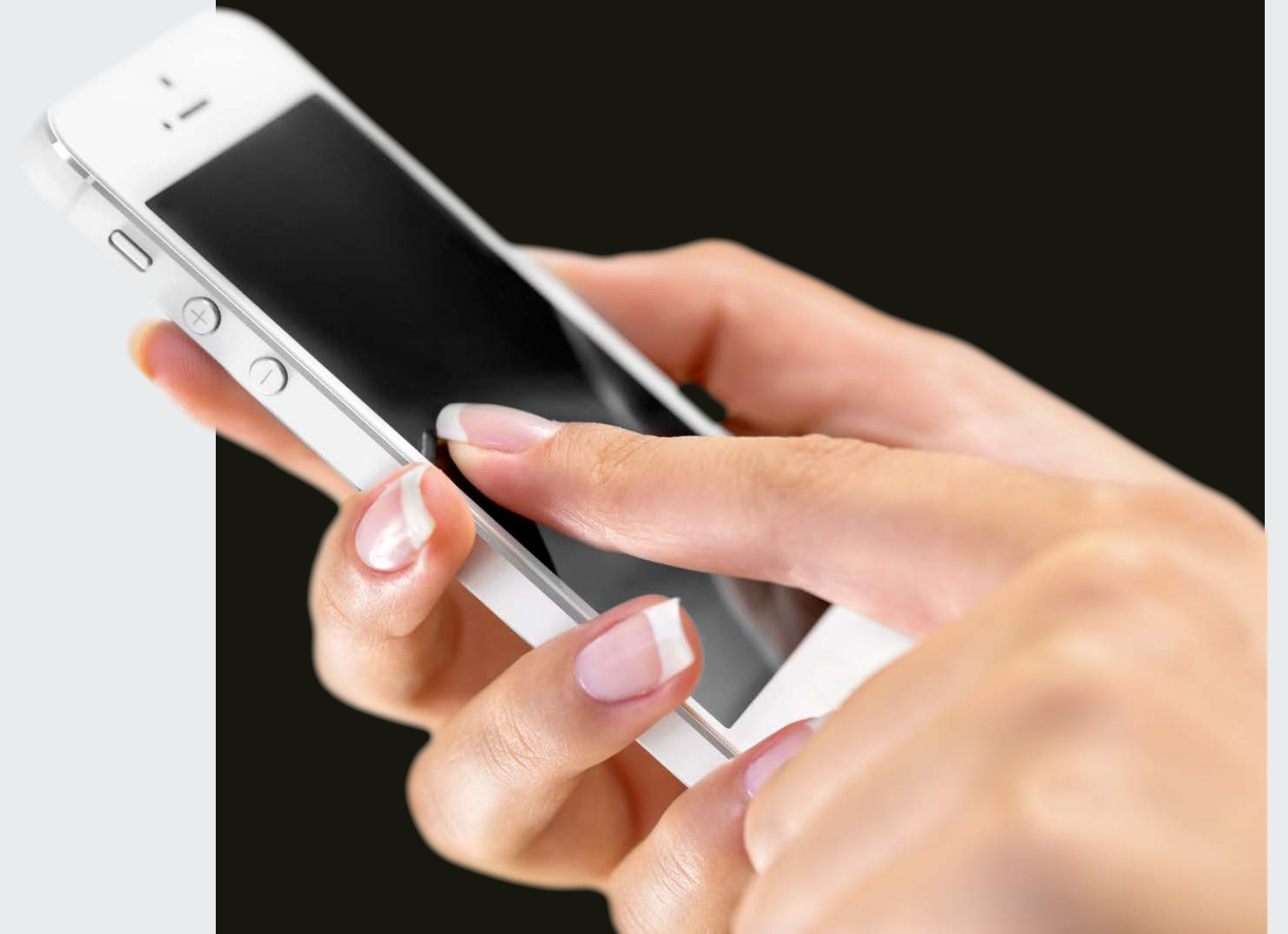
Do Not Sell Signals

Affirmative selection of an opt-out choice is no longer required. Privacy settings can signal opt-out by default.

Significance?

- Guidance gave insight into how the AG was going to interpret the very broad definition of personal information.
- Whether info was "personal info" appeared to depend on it if was actually linked to a "particular consumer or household." Linkable to a device only maybe not sufficient?
- Potentially a big loophole for a lot of relevant personal data.

Guidance on
Personal
Information



NOTICE OF RIGHT TO OPT-OUT

1

Locations

- Website homepage or download/landing page of app.
- Offline notice in prominent location.

2

Content

- Description of rights
- Webform to submit request
- Instructions for other methods to submit
- Proof required when using agent
- Link to privacy policy.

3

Notice Exemptions

No opt-out notice if business does not, and will not, sell personal info during the time period during which the notice of the right to opt-out is not posted and privacy policy reiterates.

PRIVACY POLICY DISCLOSURES



List 1

Categories of personal information the business has collected about consumers in the preceding 12 months.



List 2

Categories of sources from which the personal information is collected.



List 3

Business or commercial purpose for collecting or selling personal information.

Removes huge burden of having to provide source and purpose for each category of data collected.

Privacy Controls

Browser plugins/settings, device settings, or other mechanisms (Do Not Track?) that communicate or signal a choice to opt-out must be treated as a valid request.

Global privacy controls:

- must clearly communicate or signal an intent to opt-out of the sale; but
- no longer must require affirmative selection by the consumer to opt-out.
- Now may be designed with pre-selected settings.



CCPA Considerations

Employees' Personal Information

Does the CCPA apply?

Yes. As follows:

- Employers must provide notice to employees at or before the point of collection about the information they will collect.
- Employees have a right to sue for damages resulting from a data breach.

Notice At Collection

Required:

- A list of the categories of personal information to be collected.
- The business or commercial purpose for which the categories will be used.

Not Required:

- A Do Not Sell link
- A Privacy Policy link

Right to Sue for Breach

The right to sue for statutory damages is limited to breach of the following information:

- First/Last Name and
 - SSN
 - Driver's License number or Gov't ID number
 - Financial account or credit/debit card number, in combination with access code/password.
 - Medical Information
 - Health Information
 - Biometric Data
- Account Log-In credentials



Industry groups to
request delay in
enforcement of the
CCPA

CCPA Enforcement

Various industry groups representing advertisers, marketers, publishers, ISPs, financial services, delivery services, transportation and others, have requested delay of enforcement until January 2, 2021.

Reasons to Delay the CCPA

COVID-19

The coronavirus presents challenges in implementing compliance measures.

CCPA

Modifications

The CCPA regulations are not yet final, and businesses need time to implement them.

Revenue Hits

It is unclear how the downturn in the economy will impact business subject to the CCPA's revenue threshold.

Response from AG's Office

“RIGHT NOW, WE'RE COMMITTED TO ENFORCING THE LAW UPON FINALIZING THE RULES OR JULY 1, WHICHEVER COMES FIRST.”

"WE'RE ALL MINDFUL OF THE NEW REALITY CREATED BY COVID-19 AND THE HEIGHTENED VALUE OF PROTECTING CONSUMERS' PRIVACY ONLINE THAT COMES WITH IT. WE ENCOURAGE BUSINESSES TO BE PARTICULARLY MINDFUL OF DATA SECURITY IN THIS TIME OF EMERGENCY.”

Source: <https://www.mediapost.com/publications/article/348885/movie-industry-newspapers-join-request-to-postpon.html>

STATE PRIVACY BILLS

FAILED BILLS

Florida H963

Hawaii SB418

Maryland HB249

Mississippi HB1253

New Jersey S2834

New Mexico SB176

Pennsylvania HB1049

Rhode Island S0234

Texas HB4518

Washington SB6281

ACTIVE BILLS

Connecticut RB1108

Hawaii HB2572/HCR225

Illinois SB2330

Louisiana HR 249

Maryland SB957

Massachusetts S120

Minnesota HF3936

Nebraska LB746

New Hampshire HB1680

New Jersey A2188

New York S224/S5642

North Dakota HB1485

South Carolina H4812

Texas HB4390

Wisconsin: AB870-872

None of the active bills are out of committee as of 3/23.

Consumer Data Privacy and Security Act

INTRODUCED BY SEN.
JERRY MORAN, R-KAN ON
MARCH 12, 2020

INDIVIDUAL RIGHTS

- Access/Portability (except small businesses)
- Accuracy/Correction (except small businesses)
- Deletion (limited application to small businesses)
- Opt-out for sensitive data
- Opt-out for specific processing

BUSINESS OBLIGATIONS

- Notice and Transparency
- Purpose limitations
- Data Minimization
- Security Requirements (consideration for small businesses)
- Privacy Programs
- Service provider obligations
- Privacy impact assessments

ENFORCEMENT

- Enforcement by FTC/AG
- Direct fining authority
- No private right of action

CDPSA Specifics

Rutan & Tucker

CONSENT REQUIREMENTS

- Explicit consent required for processing sensitive data and transferring data to third parties.
- Exception for specific purposes, providing services, prevent fraud.

DATA SECURITY

- Reasonable security, vulnerability assessment, corrective action.
- Comprehensive data security program with training.

ENFORCEMENT

- Appointment of at least 440 staff to enforce the law.
- Fines of up to \$42,530 per violation per individual.

SMALL BUSINESS

Within past 6 months:

- Fewer than 500 employees
- Less than \$50Mavg. gross receipts over past 3 years
- Processes data on fewer than 1Mindividuals (or sensitive data of 100k)

SPECIFIC PURPOSE FEDERAL BILLS

Do Not Track Act (Sen. Hawley, R-MO)

Covered entities prohibited from collecting, repurposing, sharing unnecessary (e.g. advertising) personal information with third parties without express consent if DNT is enabled.

Facial Recognition Bills

- Prohibits use of facial recognition technology in absence of affirmative consent.
- Required warrant to use facial recognition to surveil individuals.

Filter Bubble Transparency Act

Requires websites using personal data to filter search results in news feeds to notify users. Requires version of news feed without use of personal information.

DASHBOARD Act

Large social media companies required to disclose data collection and value of data. Individual right to request deletion of data.



Working from Home

Privacy and Data Security Issues In a Pandemic

The COVID-19 pandemic has highlighted privacy and security concerns for businesses offering remote capabilities.

AREAS OF CONCERN

1

Malware

Malware is being packaged in "health" notices and campaigns, exploiting curiosity around COVID-19.

2

Phishing

Uncertainty and disruption to business operations creates opportunities for human manipulation.

3

Remote Access/BYOD

Work from home creates uncertainty and unfamiliarity with InfoSec. Pressure to ease security requirements for ease of access.

4

Business Interruption

Interruption to businesses via loss of productivity, breach of contract, or impossibility.

Remote Access

Legal Considerations

Compliance with Law

Remote access security must be compliant with the law. Be sure to assess remote access within "reasonable" security standards and any specific requirements.

Consistency with Public-Facing Policy

Ensure that work from home policies don't result in violation of public facing privacy/security policies.

Data Breach Considerations

Businesses are responsible for BYOD or non-business-owned devices that contain personal information that are breached.

Contractual Requirements

Vendors should ensure that shifts to remote access and/or work from home don't violate contractual provisions with businesses. Businesses should ensure that their vendors maintain security even with WFH.



Recommendations

Ensure remote access server security

See NIST SP 800-123, Guide to General Server Security

Remote access security placement

Place remote access servers at the network perimeter.

Authentication

Remote access servers should authenticate each teleworker before granting any access to the organization's resources, and then use authorization technologies to ensure that only the necessary resources can be used.

Encryption

Communications passing over the internet that contain sensitive information should be encrypted.

Inventory

Inventory of non-business owned devices to ensure that access to server is limited to authenticated users.

FEDERAL GUIDANCE

NIST SP 800-46 Rev. 2
GUIDE TO ENTERPRISE
TELEWORK, REMOTE
ACCESS, AND BRING YOUR
OWN DEVICE (BYOD)
SECURITY

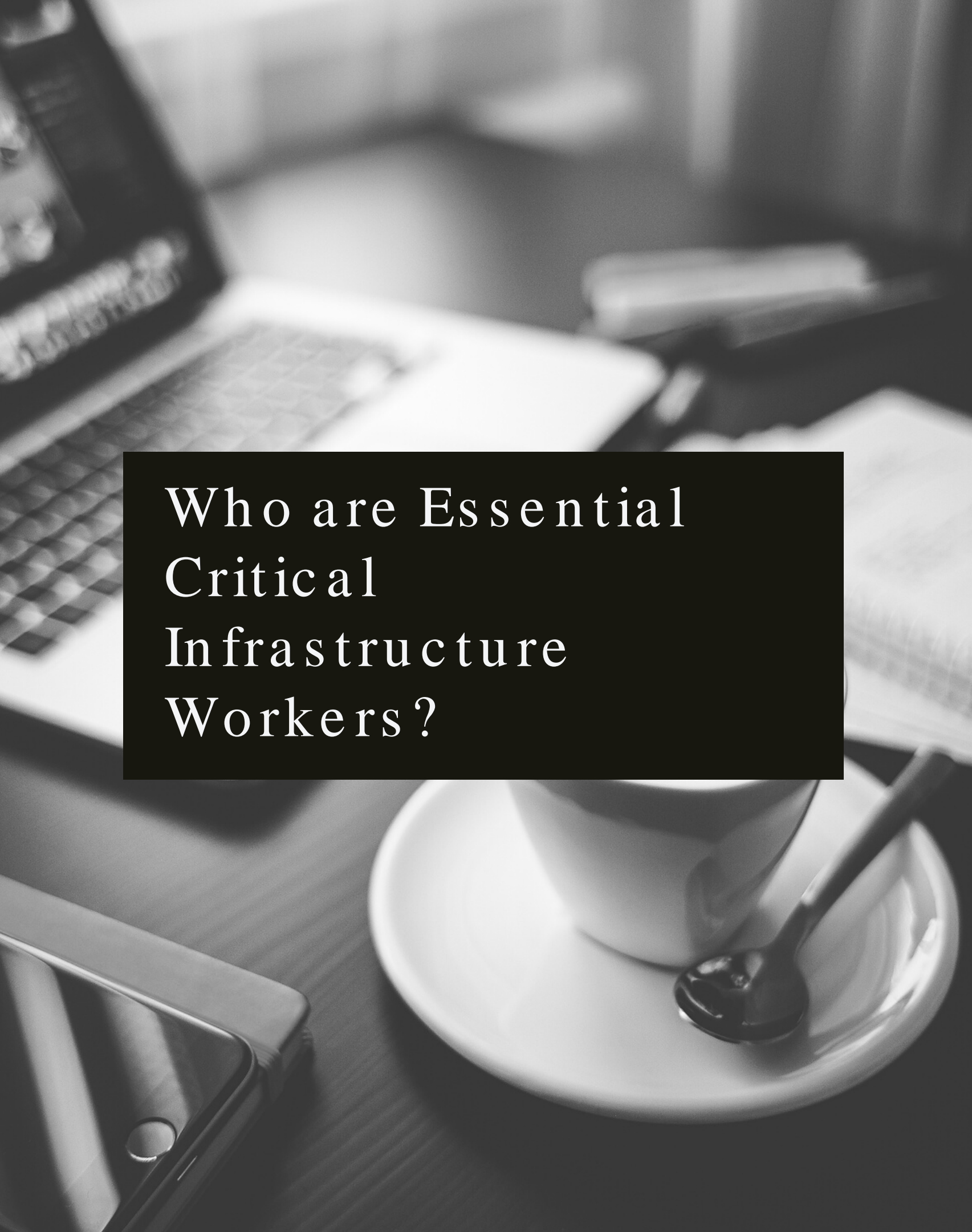


COVID-19 and Cybersecurity

Governor Newsom's Executive Order N-33-20

Application of the executive order to privacy,
cybersecurity, and other technology workers





Who are Essential Critical Infrastructure Workers?

Essential Workers

- Health Care
 - Workers performing **cybersecurity functions at healthcare and public health facilities**, who cannot practically work remotely.
 - Workers performing **security, incident management, and emergency operations** functions at or on behalf of healthcare entities including healthcare coalitions, who cannot practically work remotely.
- Communications/Information Technology
 - Data center operators, including system administrators, HVAC & electrical engineers, security personnel, IT managers, data transfer solutions engineers, software and hardware engineers, and database administrators.
 - Client service centers, field engineers, and other technicians supporting critical infrastructure, as well as manufacturers and supply chain vendors that provide hardware and software, and information technology equipment (to include microelectronics and semiconductors) for critical infrastructure.
 - **Workers responding to cyber incidents involving critical infrastructure**, including medical facilities, SLTT governments and federal facilities, energy and utilities, and banks and financial institutions, and other critical infrastructure categories and personnel.
 - Workers supporting the provision of essential global, national and local **infrastructure for computing services** (incl. cloud computing services), business infrastructure, web-based services, and critical manufacturing.
 - Workers supporting communications systems and information technology used by **law enforcement, public safety, medical, energy and other critical industries**.
- Other Essential Workforce
 - Security staff to maintain building access control and physical security measures.
 - Workers at operations centers necessary to maintain other essential functions.

<https://covid19.ca.gov/img/EssentialCriticalInfrastructureWorkers.pdf>

Vendor Agreements

COVID-19 presents unique questions with respect to contractual liability for vendors related to their failure to comply with privacy and security contract terms during the pandemic.



Vendor contracts

Questions to consider

Force Majeure

Would the force majeure clause excuse the vendor's performance of its obligations to provide reasonable security, service levels, or maintain privacy?

Loss Mitigation

If a data processing vendor ceases operations, do you have protection from data loss, theft?

Insurance

Do contractual insurance requirements protect against risk associated with vendor breach?

TIME TO REVIEW ...

1

Insurance documents

Do your policies provide coverage for anticipated losses or threats? Will a change in operation affect cybersecurity coverage?

2

Public-facing policies

Has your altered operational practices altered the veracity of the claims you make in your privacy and security policy terms? Are you still providing "reasonable" security?

3

Internal Policies

Are your internal policies consistent with the amended status quo of work from home operations? Is it time to revise them?

4

Vendor contracts

Do you know your vendors and where they stand now regarding COVID-19 and data security/privacy? Can you protect vulnerable data from ill-prepared vendors?

PERSONAL PRIVACY CONCERNS FROM COVID-19



Big Data Surveillance

South Korea, Italy, Israel: surveillance footage, device location data, credit card purchases used to track coronavirus patients to establish transmission chains.



Student Privacy

Remote learning requires data processing of minors/students. Have schools/service providers ensured legally required student privacy?



Medical Privacy

Secretary of HHS waived certain HIPAA requirements including restrictions on speaking to family/friends without consent, providing notice of privacy practices, etc.

Sources: Big Data: <https://www.nytimes.com/2020/03/23/technology/coronavirus-surveillance-tracking-privacy.html>)

HIPAA: <https://www.hhs.gov/sites/default/files/hipaa-and-covid-19-limited-hipaa-waiver-bulletin-508.pdf>

Contact Us

We'd love
to hear
from you!

Rutan's COVID-19 Task Force

611 Anton Blvd. 14th Floor, Costa Mesa, CA
92626

Phone

714-662-4691

Email

mhellbusch@rutan.com