



The Current Privacy Landscape:

Security and Privacy regulations are here to stay. Plan for them to get worse.

Technologies/ methods to protect customers/ consumers data, help your organization stand out and create new opportunities

Leon Ravenna

Chief Information Security Officer

CISSP, CIPP /C /E /G /US, CIPM, FIP, PMP

Takeaways

Where are the Hot Spots?

What Comes Next?

What to Include In Your Program

Background Primer - reference

- GDPR
- CCPA
- What about a Federal law?
- Cookies: A New Cottage Industry
- Reference Materials



Powering the world's most trusted automotive marketplaces

FOOTPRINT



75+
countries



200+
locations



15K
employees

VOLUME



3.5M
vehicles sold



~54%
vehicles
sold online



\$2.5B
revenue

VALUE



**Online
Leadership**



**Digital
Focus**



**Industry
Expertise**



Where are the
Hot Spots?



Doesn't it Seem Odd?

People give away personal data for an “app”

Will tell their innermost secrets to all their friends and their friends and so on....

Take all kinds of pictures for all the world to see

However,

Privacy is Huge





Key Security & Privacy regulations around the world

Many states/ countries not covered yet. So, expect new laws globally



How to Think About Security & Privacy

Security:
Lock the Door

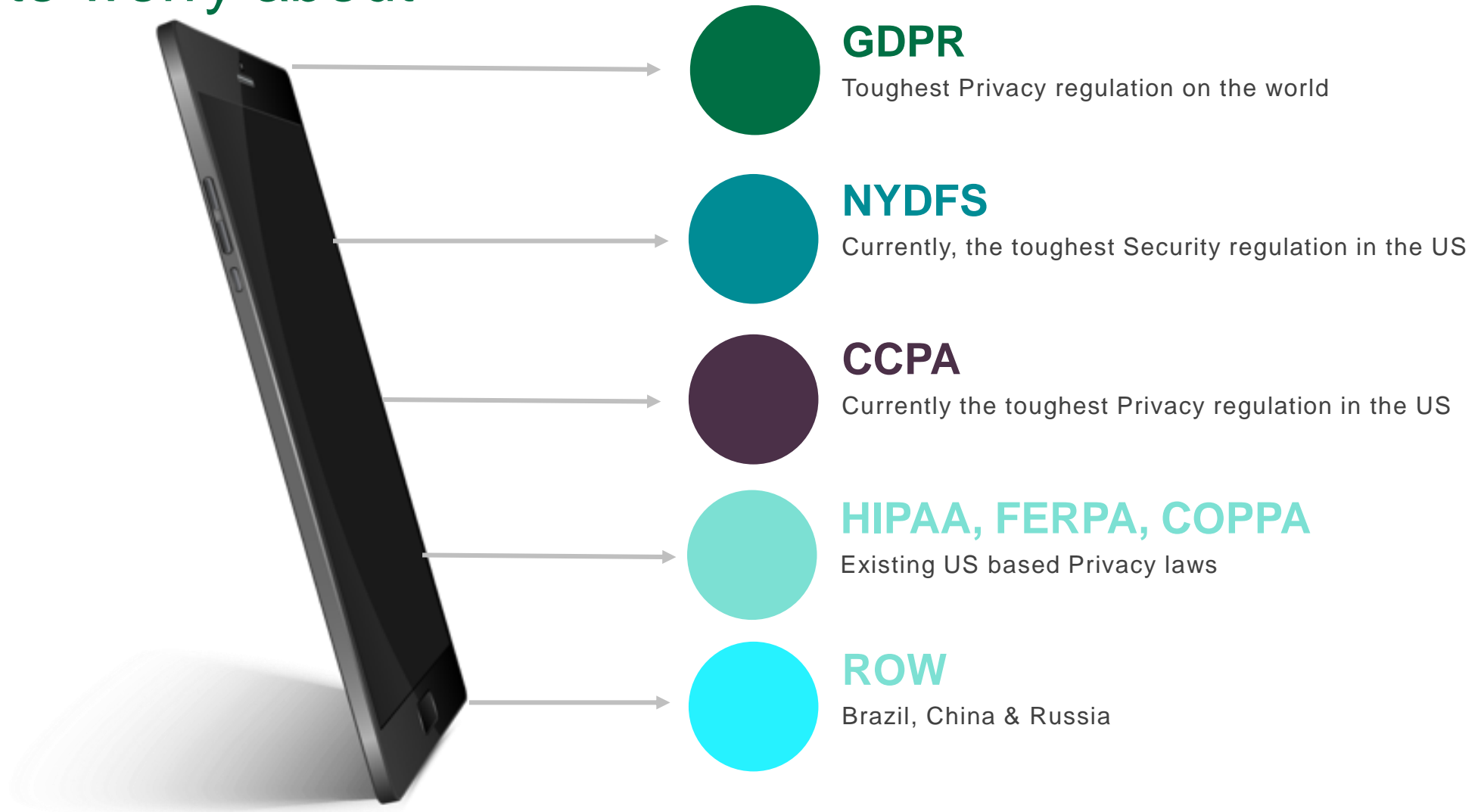


Privacy:
Close the
Shades



The Laws as we Know Them

Things to worry about



What Type of Data is Important?

GDPR Personal Data: **impacts customers**

- any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an **identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;**

GDPR Sensitive Data: **typically impacts employees**

- Processing of personal data revealing **racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership,** and the processing of **genetic data, biometric data** for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's **sex life or sexual orientation** shall be prohibited.

CCPA: Adds in the following

- Real name, alias, postal address, unique personal identifier
- Online identifier, **Internet Protocol address**, email address
- Account name, **social security number, driver's license number, passport number**, or other similar identifiers.



Recent Developments

Google – pro-business finding on Right to be Forgotten outside of the EU

Facebook – must take out content globally

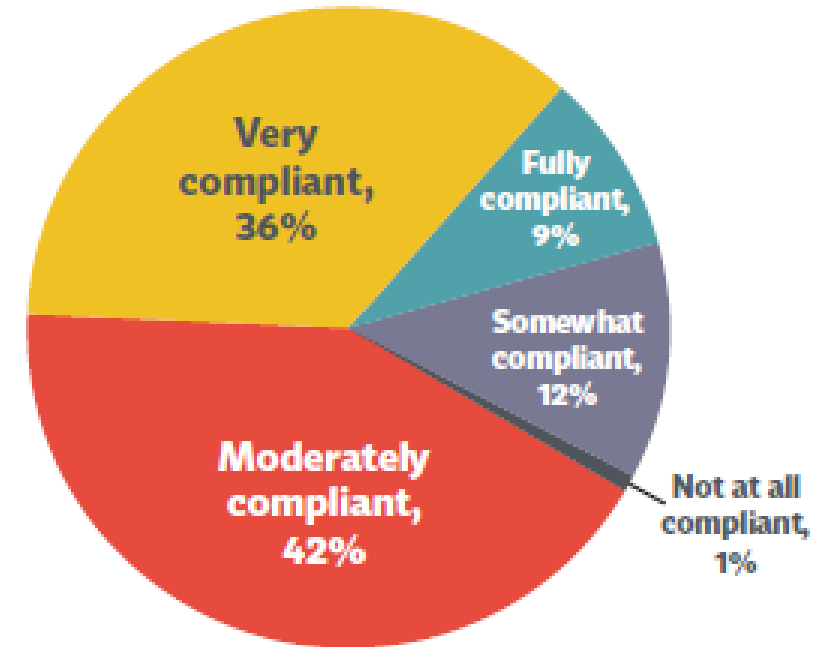
Lloyd vs. Google

- Class Action available for exposed items such as email address

Must add TTL (time to live) to cookie description

In the EU Google Analytics is now a “bad thing”

GDPR Compliance Status
(Base: must comply with the GDPR)



Published 2019-09-24 - IAPP-EY Annual Privacy Governance Report 2019, available at iapp.org - these reproductions came from their report



Fines – Thus far

HIPAA – Fairly low so far

EU in general against Google 2.7B

GDPR

Marriott – \$123m

British Airways – \$230m

FTC

Facebook – FTC fined \$5B

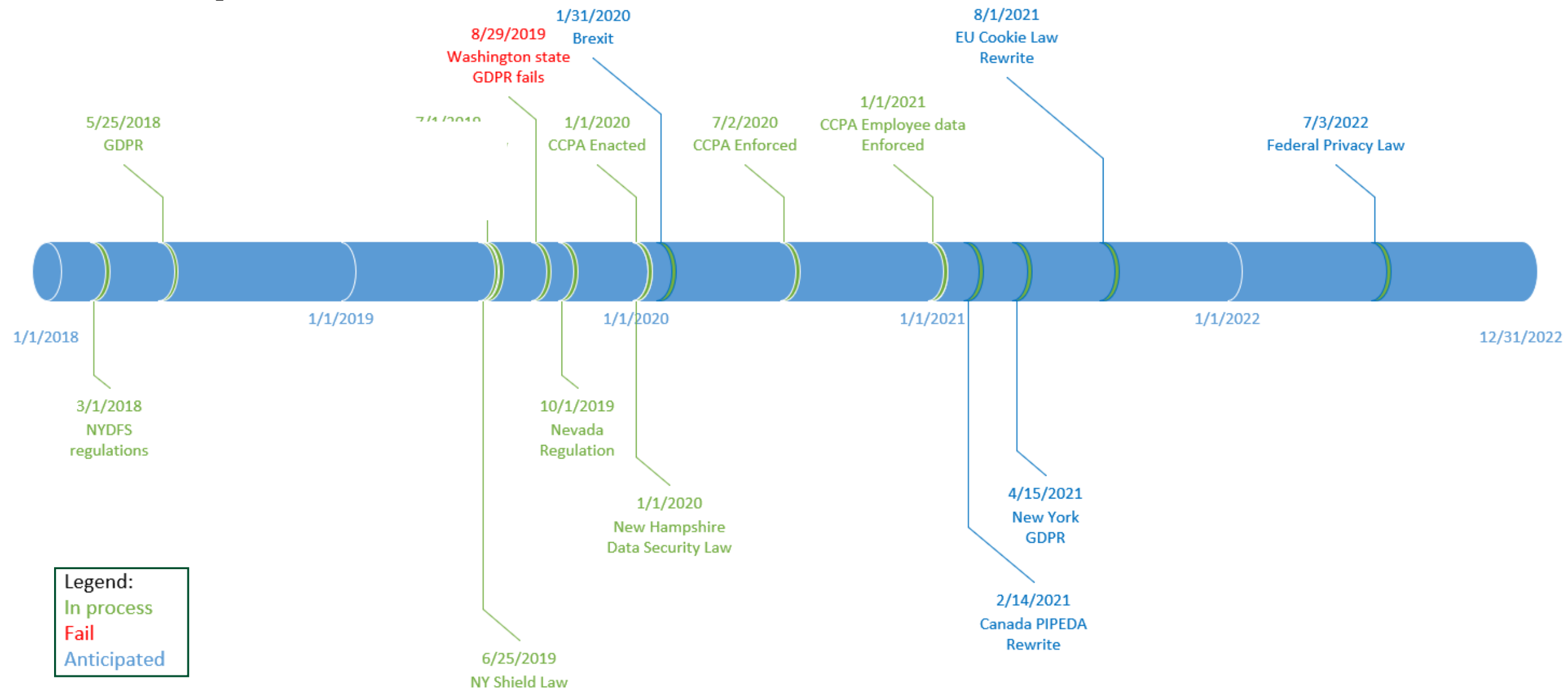




What Comes Next?



Anticipated Timeline



Post-Privacy Shield

3 ways to “cover” data transfer from the EU to the US

- Binding Corporate Rules – Rules the organization lives by (expensive and long)
- Standard Contractual Clauses (mandatory clauses that can’t be changed)
 - https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en
- Privacy Shield – EU-US agreement on data transfer

Privacy Shield was invalidated in July 2020

- EU is “scared” of US surveillance capabilities
 - No mention of similar capabilities for UK, Germany, France, etc.
- Expect BCRs and SCCs to suffer the same fate as they are contractual based

How to address for your Privacy program

- Plan to enhance Due Diligence efforts
- Is your program Defensible? Pragmatic?
- Plan to enhance documentation for data elements, data mapping, processors
- Unfortunately, expect to be told it isn’t enough



Post-Brexit

Brexit happens 1/1/2021

- Expect for UK to be treated as the US
- Just another 3rd country with no adequacy
- EU will all the sudden be “scared” of UK surveillance capabilities
 - Expect the first issue to be UK CCTV usage

How to address for your Privacy program

- Plan for the exact same things as Privacy Shield
 - Plan to enhance Due Diligence efforts
 - Is your program Defensible? Pragmatic?
 - Plan to enhance documentation for data elements, data mapping, processors
 - Take a very hard look at Controller/ Processor agreements
 - Do you have SCCs in place already?, If not, plan to implement for anything outside of UK
 - Might as well plan to add them to ALL contracts
 - Unfortunately, expect to be told it isn't enough



CCPA – CPRA and beyond

CPRA is on the ballot in November

- Plan for it to pass
- When asked the question “Do you want additional Privacy protections?” why would CA voters say No?
- CCPA-> CPRA= GDPR+

Business Obligation ...	GDPR	CCPA	CPRA
Privacy Policy Disclosure	✓	✓	✓
Data Protection by Design and Default	✓	✗	✓
Written Contracts with Processors / Service Providers / Contractors / Third Parties	✓	✓	✓
Maintain Records of Processing Activities	✓	✗	✓
Respond to Rights Requests	✓	✓	✓
New Homepage Links Required (e.g. do not sell/share personal information, limit use of sensitive personal information)	✗	✓	✓
Implement Appropriate Security Measures	✓	✓ *	✓
Security Breach Notification	✓	✓ *	✓ *
Data Protection Impact Analysis	✓	✗	✓
Data Protection Officers	✓	✗	✗
Adhere to the Rules of Cross-Border Data Transfers	✓	✗	✗

* = implied via other California law(s)



New Laws - Going Forward

Best option for success - “Blend” features of GDPR/ CCPA/ CPRA

- Do it now for best competitive advantage with other states/ localities
- This method anticipates future changes in other countries
- Adjust, don't rebuild





What to Include In Your Program

A Blended Approach

It will be remarkably difficult to address regulations on a one-off basis

The home page alone will look like a Ransom Note

- Do Not Sell
- What Data is Held
- Mandatory Consent
- Cookie Banners
- Etc., Etc., Etc.

Focus on Blended Approach

- 3 parts – GDPR (60%), CCPA (25%), NYDFS (15%) for security aspects
- Provides capability to Adjust, Not rebuild



Build to be Pragmatic & Defensible

GDPR

- ❖ Privacy Notice updates
- ❖ Data Sovereignty (data stays in EU)
- ❖ Data Mapping, DPIAs
- ❖ Cookie Banners, Privacy Preference Center
- ❖ Consent (Opt-In) tracked
- ❖ DSARs (complaints)
- ❖ RTBF/ Data Portability available
- ❖ Legal agreements (DPAs)
- ❖ Privacy Shield (HR & Consumer data)
- ❖ Security & Privacy by Design
- ❖ Strict Breach Notification SLAs

CCPA

- ❖ Privacy Notice Updates (WCAG 2.1)
- ❖ Data Mapping
- ❖ Links on sites - don't sell my data, what data is held
- ❖ **Do Not Track**
- ❖ *Optional - Cookie Banners, Privacy Center*
- ❖ *Optional - Consent (Opt-In)*



Add Security for Competitive Advantage

- ❖ Encryption: At-Rest (AES-256) & In-Transit (TLS1.2)
- ❖ Automated Key Rotation
- ❖ Consistent Password Policy
- ❖ Multi-Factor Authentication enabled for customers & employees
- ❖ PCI compliance w/ fraud detection
 - ❖ Outsource your credit card processing
- ❖ WAF & DDoS protection enabled
- ❖ All transactions logged
- ❖ Routine Vulnerability Scanning & Penetration Testing
- ❖ Strict Breach Notification Events & SLAs
- ❖ Notification of any profile change
- ❖ Security by Design
- ❖ Detailed documentation of platform
- ❖ Detailed documentation of data elements
- ❖ Failover between countries as desired



Benefits to your Company

1

Blend GDPR/ CCPA/ NYDFS

- Avoid significant fines, Public scrutiny

2

Reduce costs and simplify operations

- Structured processes require fewer resources

3

No single point of failure (auto-failover)

- Proactive approach saves time/ resources

4

Services scale with needs

- Prepare for upcoming laws (Florida , NY, FCC, SEC)
– adjust don't rebuild

5

Reduce costs and simplify operations

- Structured processes require fewer resources



Background Primer





General Data Protection Regulation (GDPR)



What Do I “Have” to Know: GDPR

Biggest Privacy Legislation ever

- Consent is huge
- Ability to Opt-out of a transaction
- Shared Liability between Controller & Processor
- Strict Breach Notification
 - Even if it isn't malicious, i.e. deletion of data

More Technical Controls

- Pseudonymization and encryption of personal data
- Proven mechanism and timing for restore of information

Certification

- You don't have to.....
- Plan on Certifying



What Do I “Have” to Know: GDPR

Data Transfer

- The US is not worthy (or adequate)
- Personal/ Sensitive data needs to stay in EEA

Transfers can only happen with “ADEQUATE” countries

- 13 countries including US (w/Privacy Shield) are adequate

Moving data

- Model Contract Clauses, BCRs, Codes of Conduct
- Derogations – limited in ability and scope

Think about your outsourcers

- Onward Transfer



What Do I “Have” to Know: GDPR

RTBF and Data Portability

- GDPR strengthens the Right to be Forgotten
- A Controller may be asked to remove all data elements
- Enhanced rights for notice & access

Breach Notification - Controller

- Notify the DPA within 72 hours
- Must notify data subjects unless data is encrypted

Sub-contractors (GDPR & Model Contracts)

- Processor must obtain authorization from Controller to sub-contract
- Processor must have contracts in place with authorized sub-contractors that meet GDPR requirements





California Consumer Protection Act (CCPA)



Tech Giants Want Uniform Privacy Law, But No GDPR

By **Ben Kochman**

Share us on:    

Law360 (September 26, 2018, 7:40 PM EDT) -- Technology giants said at a U.S. Senate hearing Wednesday that they would embrace new federal privacy legislation in the wake of headline-grabbing data misuse scandals, but urged Congress to use a lighter touch than regulators have in Europe where a strict privacy regime went into effect in May.

Representatives of six tech and telecommunication firms told the Senate Committee on Commerce, Science and Transportation that they would help craft a uniform federal privacy law that would take priority over recently enacted state laws like California's recent **Consumer Privacy Act**. But the companies warned that the end result should not mirror the EU's General Data Protection Regulation, which several firms argued had stifled innovation with its time-consuming compliance obligations.

"We encourage Congress to ensure that additional overhead and administrative demands any legislation might require actually produce commensurate consumer privacy benefits," said Andrew DeVore, Amazon's vice president and associate general counsel. Meeting the GDPR's requirements for handling, retaining and deleting personal data "required us to divert significant resources to administrative and record-keeping tasks and away from invention on behalf of customers," he added.

Representatives from [Google LLC](#), [Amazon.com Inc.](#), [Apple Inc.](#), [Twitter Inc.](#), [AT&T Inc.](#) and [Charter Communications Inc.](#) all said they would support some sort of privacy law that would give consumers more control over the way in which their data is used. But only Rachel Welch, Charter's senior vice president for policy and external affairs, said her company would support a blanket "opt-in" rule by which users would need to actively consent to the use of their personal data before companies collected it. One central pillar of the GDPR calls for companies to obtain such consent in cases where there is no other legal basis for collecting the data.

"Consumers should be empowered to have meaningful choice for each use of their data," Welch told the lawmakers. "This means no more pre-ticked 'boxes,' take-it-or-leave-it offers and no more default consents."

 Add to Briefcase
 Printable Version
 Rights/Reprints
 Editorial Contacts

Related

Sections

Consumer Protection	
Corporate	
Cybersecurity & Privacy	
Media & Entertainment	
Public Policy	
Retail & E-Commerce	
Technology	
Telecommunications	

Companies

AT&T Inc.	
Amazon.com Inc.	
Apple Inc.	
Charter Communications Inc.	
Facebook	
Google Inc.	
Twitter Inc.	

Government Agencies

Federal Trade Commission	
U.S. Senate	



Check out Law360's new podcast, Pro Say, which offers a weekly recap of both the biggest stories and hidden gems from the world of law.



Ultimately, the Tech Giants will not win out

CCPA: Key Requirements

Biggest Privacy Legislation in the US

- 60-65% of GDPR
- Right to Deletion
- Specific links to add to a website
 - Right of individual to object to selling their personal data
 - Right of individual to know what data a company holds

Fines

- Determined by CA Attorney General and up to \$7500/violation

Larger sets of personal and sensitive data

Must know what data is “sold” to 3rd parties and provide downstream protection

Individuals must to request every 12 months



CCPA Recent Developments

Enforcement started 7/2/20

Employer provisions in effect 1/1/21

“New” Proposed Rules from the California AG

- Consent will get tougher
- Mandated Do Not Track
- WCAG 2.1 for Privacy Notices
- Final rules confirmed August, 2020
 - <https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/oal-sub-final-text-of-regs.pdf?>

Expect CPRA on the ballot in November





What about a
Federal Law?



Inside Privacy

Updates on developments in data privacy and cybersecurity

FROM COVINGTON & BURLING LLP

[HOME](#) > [DATA PRIVACY](#) > WYDEN INTRODUCES MIND YOUR OWN BUSINESS ACT OF 2019

Wyden Introduces Mind Your Own Business Act of 2019

By Inside Privacy on October 21, 2019

POSTED IN [DATA PRIVACY](#)

On October 17, Senator Ron Wyden introduced in the Senate a privacy bill that would expand the FTC's authority to regulate data collection and use, allow consumers to opt out of data sharing, and **create civil and criminal penalties for certain violations** of the Act.



US Privacy Law – Coming Soon, Maybe

Issues

- Private Right of Action
- Existing Privacy Laws
- Unwillingness to mandate that states comply – may not override CA

Congress has to agree on something....

- Nothing this year – election year
- Nothing next year – The losing party will NOT be willing to work together
- 2022 is the earliest I can see
- Security components will be high

What to expect?

- States will drive their own interpretation
- 800.53 R5 will incorporate Privacy, NIST Privacy Framework Core v1.0
- Be prepared to have different states drive their own components
 - Either “one-up” or embrace GDPR





Cookies:
A New Cottage
Industry



Cookies: The New Frontier??

Cookies are becoming their own cottage industry (legal, technical, etc.)

The following are things to about:

- While not mandatory yet, expect it in 12-18 months in US
- Do you have a way to implement? In 21 languages?
- Can you implement Do Not Track?
- Can you enforce:
 - Implied Consent
 - Cookie Wall
 - User Preferences



LOGIN

Register

Login

Username



Password



All cookies are
turned off until
banner interaction
occurs

Ability to force user interaction
before site access

We use cookies to personalise content and internal ads, to provide social media features and to analyse traffic to this site. We also share information about your use of our site with our social media, advertising and analytics partners.

You can view our cookie policy, including information on exercising your rights to withdraw consent. [Cookie Policy](#)


[> Cookie Settings](#)[✓ I Accept Cookies](#)

© ADESA Global All Rights Reserved 2019



User is presented with Cookie Policy, Settings and acceptance.
Can force banner interaction before site usage as/if needed.

Privacy Preference Centre



Privacy Preference Centre

Your Privacy

Strictly Necessary Cookies

Performance Cookies

Targeting Cookies

More Information

Performance Cookies

These cookies allow us to count visits and traffic sources so we can measure and improve the performance of our site. They help us to know which pages are the most and least popular and see how visitors move around the site. All information these cookies collect is aggregated. If you do not allow these cookies we will not know when you have visited our site, and will not be able to monitor its performance.

Cookies used

_gat_gtag_UA_124907786_1, _ga, _gid

☒ **Active**

Powered by [OneTrust](#)

Save Settings

User has control at Cookie acceptance or on any future return

Will add Cookie length

Reference Materials

DLA Piper Privacy Website:

https://www.dlapiperdataprotection.com/#handbook/law-section/c1_IN

Privacy Shield

<https://www.privacyshield.gov/Program-Overview>

GDPR

http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf

ePrivacy Regulation(2002/58/EC)

<http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32002L0058&from=EN>

New ePrivacy Regulation (2002/58/EC replacement)

<https://ec.europa.eu/digital-single-market/en/news/proposal-regulation-privacy-and-electronic-communications>

Model Contract Clauses

http://ec.europa.eu/justice/data-protection/international-transfers/transfer/index_en.htm



About the Author

Leon has over 30 years' experience in Healthcare, Financial Services and Technology companies leading Global Security Strategy, Execution, Privacy and Compliance services.

Leon is currently CISO of KAR Global. A \$2.5B multi-national company in the auto auction and financial services space. He provides Security, Privacy & Compliance expertise for over 10,000 employees. Leon has led nationwide support, Web & CRM development efforts, data center builds, heavy infrastructure for SaaS companies in the medical and financial space.

Leon has extensive experience in Regulatory, Compliance & Privacy areas having managed ISO27001, HIPAA, SSAE-18, PCI and NIST system builds and audits.

In addition to holding a CISSP and PMP, Leon is one of a very small group world-wide to hold 5 major Global Privacy certifications in Privacy Management, Canadian, EU, US, US Government Privacy and is Fellow in Information Privacy.

Questions/ comments:

leon.ravenna@karglobal.com or leon.ravenna@outlook.com

