SAUSAGE MAKING IN PRIVACYLAND
The California Consumer Privacy Act of 2018 and the Credit Reporting Provisions of S. 2155

Privacy and Data Security Subcommittee of the Consumer Financial Services Committee
ABA Winter Meeting, Turnberry Isle, Miami, FL
January 13, 2019, 8:30 AM
PANELISTS

- LAURIE BABINSKI
  ASSOCIATE GENERAL COUNSEL, CREDIT KARMA, INC.

- MARC CARLSON
  VICE PRESIDENT, LEGAL, EXPERIAN NORTH AMERICA

- RITA HEIMES
  GENERAL COUNSEL, INTERNATIONAL ASSOCIATION OF PRIVACY PROFESSIONALS (IAPP)

- CHRISTOPHER OTT
  PARTNER, DAVIS WRIGHT TREMAINE, LLP

- DAVID STEIN (MODERATOR)
  OF COUNSEL, COVINGTON & BURLING, LLP
AGENDA

- The California Consumer Privacy Act of 2018
  - History, timeline, and what’s next
  - Scope and definitions
  - Key requirements
  - Exceptions
  - Enforcement
  - Compliance considerations
  - Issues to watch

- The Credit Reporting Provisions of S. 2155
  - National security freeze
  - Veteran and servicemember protections
  - GAO report
THE CALIFORNIA CONSUMER PROTECTION ACT OF 2018 OR CCPA
CCPA AGENDA

- History, timeline, and what’s next
- Scope and definitions
- Key requirements
- Exceptions
- Enforcement
- Compliance considerations
- Issues to watch
CCPA HISTORY, TIMELINE, AND WHAT’S NEXT
It all started with a ballot initiative.

- In California, a ballot proposition can be submitted to the electorate for a direct vote. To qualify, the initiative must be supported by 356,800 signatures (5% of the population that voted in the last gubernatorial election) and submitted to the Attorney General with a filing fee (Cal. Const., art. II, § 8(b); Elections Code § 9035).

- The ballot initiative was spearheaded by: Rick Arney, a finance industry executive; Alastair Mactaggart, a real estate developer; and Mary Stone Ross, a former Central Intelligence Agency analyst.

- In December 2017, a San Francisco-based consumer group known as Californians for Consumer Privacy began gathering signatures for a ballot initiative it had drafted.

- The initiative proposed broad new privacy rights even more expansive than the resulting CCPA legislation (including a more expansive definition of “sale” and a broader private right of action).

- In early May 2018, the Californians for Consumer Privacy submitted 629,000 signatures to the state, twice the number required for the initiative to be included on the November 2018 ballot.
Laws enacted through a ballot measure are very difficult to amend in California.

In mid-May 2018, State Senator Robert Hertzberg and Assemblymember Ed Chau reached out to the Californians for Consumer Privacy to see if they would withdraw the ballot initiative if California passed a privacy law addressing their concerns.

- The group agreed, but gave the legislature only until June 28, 2018 to act -- the statutory deadline for withdrawing the ballot initiative.

On June 25, 2018, Secretary of State Alex Padilla qualified the ballot initiative.

The state legislature passed the law just before the deadline; Governor Jerry Brown signed it into law on June 28, 2018 with effective date of January 1, 2020.
The California legislature adopted technical or “clean-up” amendments (SB 1121) on August 31, 2018. Preceded by intense negotiations.

Changes to certain exceptions.
- Important clarification and expansion of GLBA exception.

Changes to enforcement provisions.
- Eliminated requirement that potential plaintiffs notify Attorney General before filing suit and AG veto authority over private lawsuits.

Changes to timing.
- Regulation deadline extended to July 1, 2020.
More legislative amendments possible
- New legislative session began December 3, 2018 (largely ceremonial).
- Legislature convenes for substantive work this month (January 2019).

Reportedly the legislature had agreed in principle to some additional changes, but the text needed to be published for a vote couldn’t be finalized before the end of the legislative session.
- Some legislators remarked when the amendments were adopted that there is more work to be done.
- Industry also noted in its letter supporting SB 1121 that there was more work to be done.

But it’s important to remember that industry and consumer advocates will both be pushing for changes, so there is risk that some things could get worse even if others get better, or legislature may await AG rules.

Attorney General will seek public feedback and adopt implementing regulations by the July 1, 2020 deadline.
POTENTIAL IMPACT BEYOND CALIFORNIA

- Other states may follow California’s lead
  - But the California process has been messy.
  - No groundswell yet at the state level.

- Federal legislation
  - Several members of Congress are working on draft privacy legislation.

- Federal regulation or oversight
  - No indication of new regulatory push by CFPB or prudential regulators.
  - Heightened privacy supervision and enforcement possible.
  - US Commerce Department is requesting public feedback on risk-based privacy principles through the National Telecommunications and Information Administration.
SCOPE AND DEFINITIONS
CONSUMER

- “Consumer” is a natural person who is a California resident (Cal. Civ. Code 1798.140(g)).

- CCPA definition is much broader than GLBA definition of “consumer.”

- Under GLBA, a “consumer” is an individual who obtains or has obtained a financial product or service from a financial institution primarily for personal, family or household purposes.
REGULATED ENTITIES: BUSINESS

- A “business” is the CCPA regulated entity.
- A “business” is a for-profit entity that collects personal information on California residents, determines the purposes and means of processing the PI, does business in California, and does one of the following:
  - Has annual gross revenues > $25M;
  - Annually buys, receives/shares for commercial purposes, or sells (alone or in combination) personal information of ≥ 50,000 residents, households, or devices; or
  - Derives 50% or more of its annual revenues from selling California residents’ personal information.
A business includes any entity that controls or is controlled by a business and that shares common branding with the business.

- Control or controlled means ownership or power to vote more than 50% of outstanding shares, control over election of directors, or control over management.
- Common branding means a shared name, servicemark, or trademark.

A business does not include:

- Two sibling companies under the common control of parent or holding company (affiliates under GLBA);
- Ownership, control, or power to vote 25% or more of outstanding shares (GLBA standard); or
- Affiliated companies that use different brands, e.g., a bank brand and a securities brand.
SERVICE PROVIDERS V. THIRD PARTIES

- A “service provider” is a for-profit entity that
  - Receives personal information from a business for a “business purpose” (as defined in the CCPA); and
  - Processes personal information on behalf of a business pursuant to a written contract that prohibits the retention, use, or disclosure of the personal information for purposes other than performing the services.

- A “third party” is an entity that is
  - Not a business; and
  - Not a service provider.
PERSONAL INFORMATION

- Broadly defined as information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household.

- Personal information includes:
  - Identifiers (individual consumer or household)
    - Includes a real name, alias, postal address, unique personal identifier, online identifier, IP address, email address, account name, social security number, driver’s license number, passport number, and other similar identifiers.
  - Data Protected under State Data Security Law
    - Includes identifying information and various types of financial, insurance, medical, and employment information.
  - Characteristics Protected by State or Federal Law
    - CA law includes 17 protected characteristics, including race, gender, marital status, national origin, and others not covered by federal law.
PERSONAL INFORMATION (CONT.)

- Personal information includes:
  - Commercial information
    - Not defined, but includes “records of personal property, products or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies.
  - Biometric information
  - Internet/electronic network activity information
    - Includes browsing history, search history, and Web site interactions
  - Geolocation information
  - Audio, electronic, visual, thermal, olfactory, or similar information
  - Professional or employment-related information
  - Education information
  - Inferences drawn from personal information to create a profile

- Personal information does not include publicly available information from government records, but only if used for a purpose compatible with the government’s maintenance and publication of such information.
KEY REQUIREMENTS
FOUR KEY REQUIREMENTS

- Data Access and Disclosure
- Data Deletion
- Opt-out of Data Sale (Opt-in for Minors)
- Non-Discrimination
A business that collects a consumer’s personal information must disclose to a consumer upon receipt of a verifiable consumer request:

- The categories of personal information collected;
- The sources of the information;
- The business or commercial purpose for collecting or selling personal information;
- The categories of third parties with whom the business shares personal information; and
- The “specific pieces of personal information” collected.

(Cal. Civil Code 1798.100 and .110)
DATA ACCESS AND DISCLOSURE
(CONT.)

A business that sells or discloses for a business purpose a consumer’s personal information must disclose to a consumer upon receipt of a verifiable consumer request:

- The categories of personal information collected;
- The categories of personal information sold (or the fact that no information has been sold) and the categories of third parties to whom the information was sold; and
- The categories of personal information disclosed for a business purpose.

(Cal. Civil Code 1798.115)
DATA ACCESS AND DISCLOSURE (CONT.)

- Businesses must respond to verifiable consumer requests to access personal information within 45 days (though they can request an extension up to ninety days). (Cal. Civil Code 1798.130(a) and .145(g))

- Disclosures must:
  - Cover the 12 months preceding the request;
  - Be provided free of charge;
  - Be delivered in writing or electronically; and
  - Be provided in a portable and (where possible) readily useable format, if provided electronically. (Cal. Civil Code 1798.100)
DATA DELETION

- A business must delete any personal information it has collected from the consumer upon receipt of a verifiable consumer request, subject to certain exceptions. (Cal. Civil Code 1798.105)

- Exceptions apply if the data is necessary to:
  - Complete a transaction or provide a service the consumer requested;
  - Engage in activities reasonably anticipated within the context of an ongoing business relationship with the consumer;
  - Protect against fraud or other illegal activity;
  - Comply with the law;
  - Engage in certain research;
  - Exercise free speech rights; or
  - Enable internal uses reasonably aligned with consumer expectations.

- A business that collects personal information must disclose to consumers the right to request deletion of that information.
**OPT-OUT OF SALE**

- Consumers have the right, at any time, to direct a business not to sell his or her personal information to third parties. This is the right to opt-out. (Cal. Civil Code 1798.120(a))

- A business must provide a clear and conspicuous link on its Internet home page titled “Do Not Sell My Personal Information” that enables the consumer to opt-out and must describe the opt-out right. (Cal. Civil Code 1798.120(b) and .135(a))

- Minors aged 13-16 must opt-in or affirmatively consent to the sale of their personal information.

- A parent or guardian must opt-in or affirmatively consent to the sale of personal information for children under the age of 13.

- “Sale” or “sell” means processing “for monetary or other valuable consideration.”
NON-DISCRIMINATION

- A business may not discriminate against a consumer for exercising any rights under the CCPA by:
  - Denying goods or services to the consumer;
  - Providing a different level or quality of goods or services to the consumer; or
  - Charging different prices based on the exercise of CCPA rights.

- A business can offer different quality services if the difference is reasonably related to the value provided by the consumer’s data.

- A business can provide financial incentives to encourage users’ participation in the collection of personal information.

(Cal. Civil Code 1798.125)
EXCEPTIONS
KEY CCPA EXCEPTIONS

The CCPA does not apply to:

- **GLBA Exception**: Personal information collected, processed, sold, or disclosed pursuant to the GLBA, its implementing regulations, or the California Financial Information Privacy Act.
  - Initial exception was narrower; CCPA had to be “in conflict” with GLBA.
  - Amended in September 2018.

- **FCRA Exception**: The sale of personal information to or from a consumer reporting agency if that information is to be reported in, or used to generate, a consumer report as defined in the FCRA, and use of that information is limited by the FCRA.

- **DPPA Exception**: Personal information collected, processed, sold, or disclosed pursuant to the Driver’s Privacy Protection Act.
Despite the GLBA and FCRA exceptions, the CCPA’s broad scope may still apply to certain personal information financial institutions collect about:

- Employees, contractors, and job applicants;
- California residents associated with business loans or accounts, such as guarantors and principals; or
- Possibly individuals browsing a company’s website without seeking a product or service.
ENFORCEMENT
TWO ENFORCEMENT MODELS

- **Privacy violations** = AG enforcement only
  - Violations of data access and disclosure, data deletion, opt-out of sale, and non-discrimination provisions.

- **Data security violations** = AG enforcement and private rights of action (individual or class actions)
  - **Standard**: Unauthorized access and exfiltration, theft, or disclosure of personal information (as defined more narrowly in CA's data breach notice law) that was not encrypted or redacted, and the breach occurred because the business failed to maintain reasonable security practices.
  - Data encryption provides a safe harbor against litigation.
  - The duty to use reasonable security measures is not new. California law requires businesses to use reasonable security measures to protect personal information of California residents. (Cal. Civ. Code § 1798.81.5)
Penalties and Cure Rights

Administrative penalties:
- No AG enforcement until either 6 months after final AG regulations (required by July 1, 2020) or July 1, 2020 -- whichever is sooner.
- Business has opportunity to cure alleged violation within 30 days of notice.
- Injunction and Civil Penalty
  - Up to $2,500 for each negligent violation; and
  - Up to $7,500 for each intentional violation.

Private action penalties:
- Prior to initiation, business has opportunity to cure alleged violation within 30 days of notice.
- Statutory damages between $100-$750 per consumer per incident, or actual damages.
- Injunctive or declaratory relief, and other relief court deems proper.
COMPLIANCE CONSIDERATIONS
DATA INVENTORY

- Consider conducting a data inventory to assess:
  - What data is collected and stored on California residents;
  - Whether it is disclosed to service providers or third parties;
  - Whether the data is sold;
  - Whether and how individuals can access/delete the data;
  - What data sources are used; and
  - Whether the data falls within an exception.

- Data mapping to GDPR requirements may provide a starting point (but the CCPA contains a broader definition of “personal information”).

- Data inventory can be done now.
STRATEGIC COMPLIANCE OPTIONS

- Consider whether to voluntarily apply CCPA rights across the US for business, administrative, or operational reasons.

- Consider data de-identification
  - Defined in, and excluded from coverage by, the CCPA.
  - De-identification/anonymization also addressed in GLBA.

- Consider using data encryption to get safe harbor from civil liability for data breaches.

- Consider updating data collection, retention, and deletion policies in California or nationwide.

- Consider whether revised verification procedures are necessary for California residents.
CALIFORNIA-SPECIFIC ACTIONS

- Update privacy policy (as applicable) to reflect CCPA disclosure requirements.
- Create a "Do Not Sell" button and related internal procedures (where applicable).
- Review template vendor agreement.
- Conduct gap assessment against other CCPA requirements (e.g., non-discrimination and encryption/data security).
- Update training programs.
ISSUES TO WATCH
**SOURCES OF ISSUE RESOLUTION**

- Further legislative amendments
- AG regulations
- AG enforcement

- Legislature may defer to AG regulations on various issues to limit amendments.
- AG enforcement resources very limited.
CALIFORNIA AG ISSUES

- The timing and substance of AG rulemakings.
- The California AG has expressed concerns with:
  - The requirement that the AG provide businesses and third parties with opinions, warnings, and opportunities to cure.
  - Impact of budgetary constraints on fulfilling CCRA responsibilities.
  - The narrowness of the private right of action. The AG wants private right of action expanded to CCPA privacy violations and not limited to data security violations.
Privacy and consumer advocates want to:

- Preserve consumers’ ability to access specific pieces of their personal information;
- Preserve consumers’ ability to obtain data in a portable and readily usable format;
- Retain the current broad definition of personal information, including household identifiers;
- Clarify that de-identified information does not include pseudonymized information; and
- Expand private rights of action to privacy violations.
Industry wants additional amendments to:

- Revise the definition of “consumer” to exclude employees and contractors;
- Narrow definition of “personal information” to remove references to household and probabilistic identifiers, inferences and tendencies, and professional or employment-related information;
- Remove or clarify access and portability requirements;
- Remove requirement for businesses to identify “specific pieces of information”;
  - Argument that keeping specific pieces of information in disclosure-ready format increases’ exposure to hackers.
INDUSTRY ISSUES (CONT.)

- Clarify the exemptions for fraud, IP infringement, and other legal purposes;
- Clarify that a business is vulnerable to personal suit only if the affected information was not encrypted and not redacted;
- Ensure that a third party is not liable for selling personal information unless the third party received notice of a consumer exercising his or her right to opt-out; and
- Clarify that the business has a reasonable amount of time to verify a consumer request.
Impact on emerging technologies

- Blockchain and artificial intelligence/machine learning technologies don’t lend themselves to individual requests for deletion and access rights.
- Applying the CCPA deletion and access rights to blockchain and AI/machine learning could hinder technology development.

Impact on First Amendment

- Potential chilling effect if reporting triggers CCPA demands.

Impact on Employment

- No exception for employment data.
- Potential for deletion or suppression of negative employment histories.
CREDIT REPORTING PROVISIONS OF S. 2155
OVERVIEW OF S. 2155

- Economic Growth, Regulatory Relief, and Consumer Protection Act (the “EGRRCPA”).
- Signed into law on May 24, 2018.
- Primarily reduces regulatory burdens on banks by modifying aspects of the Dodd-Frank Act.
- Amends the Fair Credit Reporting Act (“FCRA”) to impose certain new credit reporting requirements on nationwide CRAs and others.
- Requires GAO report on the credit reporting system.
KEY FCRA CHANGES

- Adopts a national security freeze (Section 301)
  - Applies to nationwide CRAs; and
  - Preempts state security freeze laws.

- Requires nationwide CRAs to suppress reporting of certain veterans’ medical debts and resolve disputes about such debts (Section 302).

- Requires nationwide CRAs to provide free electronic credit monitoring to active duty military consumers (Section 302).

- Gives consumers the right to request a financial institution delete a reported default on a private student loan if the FI offers and the consumer meets certain conditions of a loan rehab program (Section 602).
NATIONAL SECURITY FREEZE
NATIONAL SECURITY FREEZE BASICS

- Creates both a national security freeze procedure and a protected consumer security freeze procedure that nationwide CRAs must follow.

- Duration of initial fraud alerts extended from 90 days to 1 year.

- Express preemption of state security freeze laws with respect to “any subject matter regulated under” the federal security freeze provisions.
  - No grandfathering of existing state freeze laws.

- Effective date of September 21, 2018.
GENERAL RULE AND EFFECT

- **General rule**: A nationwide CRA must place a security freeze on the consumer’s file, free of charge, upon a direct request of the consumer and receipt of proper identification.
  - **Timing**: Place freeze within 1 business day after request by toll-free telephone or secure electronic means or 3 business days after request by mail.
  - No requirement to notify other CRAs; no tri-bureau centralized source for security freezes.

- **Effect**: Placement of a security freeze generally prohibits a nationwide CRA from disclosing the contents of a consumer report subject to the freeze to any person requesting a consumer report.
EXCEPTIONS ALLOWING DISCLOSURE

- Despite a security freeze, exceptions allow the disclosure of consumer reports for the following purposes:
  - Account review or collection purposes
  - Making firm offers of credit or insurance
  - Providing credit monitoring services to the consumer
  - Fraud prevention
  - Identity verification not connected with granting credit
  - Insurance underwriting
  - Employment, tenant, and background screening
  - Complying with a court order or subpoena
  - For certain government purposes
**PROCEDURAL PROVISIONS**

- **Confirmation:**
  - Send confirmation to the consumer not later than 5 business days after placing a security freeze; and
  - Tell the consumer how to remove the freeze and opt out of prescreened solicitations.

- **Removal:** Security freeze can be removed
  - If based on material misrepresentation of fact by the consumer, or
  - Upon the consumer’s direct request, free of charge, within 1 hour of a request by toll-free telephone or secure electronic means or 3 business days of a request by mail. Consumer may specify temporary removal for a specified period of time.

- **Webpage:** Nationwide CRA must establish a webpage that allows a consumer to request a security freeze, initial or extended fraud alert, or active duty alert, or opt out of prescreened offers. The webpage cannot be the only mechanism for requesting a security freeze.

- **Notice:** Add statutory security freeze notice to Section 609 summary of rights.
A protected consumer is an individual under the age of 16 at the time of the request or an incapacitated person or a person for whom a guardian or conservator has been appointed.

Most provisions similar to the national security freeze with certain variations.

Security freeze applies both to a consumer report, and, for a protected consumer with no credit file, to a “record” created by the CRA for the sole purpose of complying with the protected consumer security freeze provision that identifies a protected consumer.
PROTECTED CONSUMER SECURITY FREEZE: GENERAL RULE

- A nationwide CRA must place a security freeze on the file or record of a protected consumer, free of charge, upon the direct request from the protected consumer’s representative within the same timeframes for the national security freeze, subject to receipt of:
  - **Sufficient proof of identification**: SSN, copy of Social Security card, certified or official copy of a birth certificate, or copy of driver’s license or other government-issued ID; and
  - **Sufficient proof of authority to act as a protected consumer’s representative**: court order, power of attorney, document showing proof of parentage (including a birth certificate), or a written communication from a county agency that the protected consumer is in foster care.
PROTECTED CONSUMER SECURITY FREEZE: EFFECT AND PROCEDURES

- **Effect:** Placement of a freeze generally prohibits a nationwide CRA from disclosing a protected consumer’s consumer report or “record” to a person requesting a consumer report.

- **Exceptions:** No exceptions like those that apply to a national security freeze.

- **Removal:** Security freeze can be removed
  - If based on material misrepresentation of fact by the protected consumer’s representative;
  - Upon the direct request of the protected consumer’s representative with proof of authority; or
  - Upon the direct request of the protected consumer, if the protected consumer is not under the age of 16 at the time of the request.
VETERAN AND SERVICEMEMBER PROTECTIONS
VETERANS’ MEDICAL DEBTS

Basics

- S. 2155 amends the FCRA to impose new obligations on nationwide CRA’s with regard to certain veterans’ medical debts.

- Addresses consumer reporting issues veterans face when the VA fails to pay or delays payment for services provided in non-VA facilities.

- A “veteran’s medical debt” is a medical collection debt of a veteran owed to a non-VA health care provider that was submitted to the VA for payment for authorized care and includes debts wrongfully charged to a veteran by the VA.

- Effective date: 1 year after date of enactment.
GENERAL RULE: SUPPRESS TRADELINES

- A nationwide CRA must suppress the reporting of any information:
  - (A) Related to a veteran’s medical debt if the services antedate the report by less than 1 year; **OR**
  - (B) Related to a fully paid or settled veteran’s medical debt that had been characterized as delinquent, charged off, or in collection; **IF**
  - The CRA has actual knowledge that the information relates to a veteran’s medical debt; and
  - The CRA uses a VA-established database (if fully functional) to verify the debt as a veteran’s medical debt.

- Within 1 year of enactment, and after notice and comment, VA must establish a database to allow CRAs to verify whether a debt is a veteran’s medical debt.
  - No apparent obligation to suppress until database functional.
A nationwide CRA must delete medical debt information from a veteran’s file and notify the furnisher and the veteran of that decision if the veteran submits:

- A notice from the VA that it has assumed liability for all or part of a veteran’s medical debt;
- Proof of liability of the VA for payment of the debt; or
- Documentation that the VA is in the process of making payment.
FREE CREDIT MONITORING BASICS

▪ Nationwide CRAs must provide free electronic credit monitoring to active duty military consumers, including members of the National Guard, who provide proof of active duty military status and contact information.
  ▪ At a minimum, must notify an active duty military consumer of a material addition or modification to the consumer’s file.
  ▪ Effective date: 1 year after date of enactment.

▪ The FTC, within 1 year of enactment, must adopt credit monitoring regulations to define an electronic credit monitoring service, material additions or modifications to the consumer’s file, and what is appropriate proof of active duty military status.
FTC PROPOSED RULE

- Issued on November 1, 2018.
- Comment period closed January 7, 2019.
- Anticipated final rule publication date: May 24, 2019.

- Appropriate Proof of Active Military Status can be achieved by
  - A copy of active duty orders;
  - Certification of active duty status issued by DoD;
  - Verification through method approved by the DoD; or
  - Certification through a method accepted by nationwide CRA.

- Material Additions defined as:
  - New accounts opened in the consumer’s name;
  - Inquiries/requests for consumer reports;
  - Changes to consumer name/address/phone number;
  - Changes to credit account limits; or
  - Negative impact items (e.g., delinquency, default, late payment).
GAO REPORT
GAO REPORT REQUIREMENT

- S. 2155 requires GAO to submit a comprehensive report within 1 year on the legal and regulatory structure for CRAs, including any gaps, the dispute process, the causes of inaccuracies, data furnisher responsibilities, CRA data security, consumer report access, control or ownership of consumer credit data, and recommendations for improving the credit reporting system (Section 308).

- “Control and ownership of consumer credit data” is a key issue for the credit reporting system.