California Consumer Privacy Act (CCPA), The European General Data Protection Regulation (GDPR) and the role of Internal Audit

Doron Rotman (Managing Director)

February 12, 2020
Your speaker

Doron Rotman
Managing Director
3975 Freedom Circle Dr.
Mission Towers I, Suite 100
Santa Clara, CA 95054
Agenda

— Opening thoughts
— California Consumer Privacy Act (CCPA): Overview
— Accelerating efforts through GDPR compliance
— Internal Audit’s role in privacy compliance
— Auditing CCPA readiness
— Questions?
Opening thoughts

— Companies expected to spend $55B in initial compliance costs
  - 500+ Employees: ~$2M
  - Fewer than 20 Employees: ~$50,000
— The law is set
  - As expected the Governor signed all seven amendments
    — Includes one-year exemption for Employees and B2B and clarifies the definition of “Personal Information” (PI)

Source:
CNBC.com, “California’s new privacy law could cost companies a total of $55 billion to get in compliance.” (https://www.cnbc.com/2019/10/05/california-consumer-privacy-act-ccpa-could-cost-companies-55-billion.html) (October 5, 2019)
Opening thoughts (continued)

— A new and revised CCPA?
  - California Privacy Rights and Enforcement Act of 2020
    — Spearheaded by the father of the CCPA would extend the CCPA
  - California Attorney General (AG) issued revised proposed regulations on February 6
    - Short comment period

Source:
CNBC.com, “California’s new privacy law could cost companies a total of $55 billion to get in compliance.” (https://www.cnbc.com/2019/10/05/california-consumer-privacy-act-ccpa-could-cost-companies-55-billion.html) (October 5, 2019)
Attorney General Becerra Publicly Releases Proposed Regulations under the California Consumer Privacy Act
Organizational view: What is the issue?

**Threat**
- Regulatory non-compliance
- Data breach, data leakage
- Adverse employee/Customer reaction (e.g., profiling, tracking)

**Impact**
- Brand
- Reputation
- Profit
- Share price
- Trust
Greater attention to privacy

— User data is both captured by devices and services and knowingly created as users engage with technology.

— Data-centric companies use data to create value. The collection of this data was previously free and unrestricted, allowing companies free access to a valuable resource.

— But that is now changing. Regulations, operational cost and changing consumer preferences are creating new barriers to companies accessing and leveraging consumer data.
Global law application

All public and private entities are covered by enforceable legislation (possibly with a few well-defined and limited exceptions).

All public or private entities are covered by enforceable legislation, or some mix or large exceptions in either category exist.

Source: Data sourced from Forrester Research 2019 Regulatory Landscape.
State Consumer Privacy Rights Regulatory Landscape

California Consumer Privacy Act (CCPA), overview
Poll the audience

— How many of you know about the CCPA?
— How many of your companies have an active enterprise CCPA initiative?
— How many of you have a planned CCPA Internal Audit? (either Pre-Jan or Post-Jan)
## CCPA Overview

<table>
<thead>
<tr>
<th>Key issues and considerations</th>
<th>CCPA</th>
</tr>
</thead>
<tbody>
<tr>
<td>Covered Entity/Applicability</td>
<td>Revenues of $25 million; or data on 50k residents/households/devices; or 50% of revenues are from selling PI</td>
</tr>
<tr>
<td>General Enforcement Power</td>
<td>California Attorney General; Private right of action (see below)</td>
</tr>
<tr>
<td>Civil Penalty</td>
<td>Per violation: Up to $7,500 (intentional); $2,500 (non-intentional)</td>
</tr>
<tr>
<td>Cure Period</td>
<td>Within 30 days of being notified</td>
</tr>
<tr>
<td>Breach Notification Timeline</td>
<td>In the most expedient time possible, without unreasonable delay</td>
</tr>
<tr>
<td>Private Right of Action</td>
<td>A consumer may bring an action to recover up to $750 per breach or actual damages, whichever is greater</td>
</tr>
<tr>
<td>Consumer Access Request</td>
<td>Requires three methods for requesting access to information, through website, telephone, and in-store</td>
</tr>
<tr>
<td>Customer Access Request</td>
<td>45 days; an extension of 45 days may also be requested (90 days total)</td>
</tr>
<tr>
<td>Do Not Sell My Personal Information</td>
<td>Permissible, as long as the value of the incentive can be reasonably linked to the value of the data provided by the consumer</td>
</tr>
<tr>
<td>Offering Incentives in Exchange for Data</td>
<td>Right to Data Portability, Opt-In Consent for Minors</td>
</tr>
<tr>
<td>Additional Consumer Rights</td>
<td>Revenues of $25 million; or data on 50k residents/households/devices; or 50% of revenues are from selling PI</td>
</tr>
</tbody>
</table>
Key CCPA considerations

— Treating all PI as if the CCPA applies throughout the US – Many companies view the rapidly evolving regulatory landscape as a reason to treat consumer PI consistently [e.g., several new privacy laws have been signed or are in varying stages of the legislative process – Nevada SB 220 (October 1, 2019); Maine LD 946 (July 1, 2020); New York Privacy Act (proposed bill); the US federal government is considering the topic, in light of the EU’s GDPR.

— Leveraging GDPR to accelerate CCPA readiness – Global companies that are subject to GDPR are leveraging their existing compliance efforts to meet new regulatory requirements including CCPA during this time of global privacy revolution.

— Where’s our data – Companies are leveraging automated data discovery tools to build a more robust data inventory and discover personal information across their environment (structured, unstructured, semi-structured; cloud, on-prem).
Key CCPA considerations (continued)

— **Drawing a line in the sand** – The scope of the CCPA extends beyond the primary system of record and covers replicated data, data backups, and unstructured data contained in spreadsheets and hard copy data; Some companies are taking a risk-based approach to their CCPA readiness activities and focusing on higher risk/volume data stores.

— **Avoiding a breach when fulfilling a consumer request** – Companies are expressing concerns in how to avoid a data breach when fulfilling a consumer request (e.g. verifying a consumer is who they say they are).
Potential CCPA liability exposure

The CCPA creates additional financial exposure to companies for breaches of PI impacting CA residents and/or violations of the law.

Enforcement Mechanisms:

— Civil Suits (Private Right of Action) for a data breach involving Consumer PI (including employees)
  - Statutory damages:
    — Penalties range from $100-$750 per incident, or actual damages (whichever is greater)
— Government Enforcement (CA Attorney General) for any violation of the CCPA
  - Penalties for a violation of the CCPA:
    — Up to $2,500 per unintentional violation & Up to $7,500 per intentional violation

Example:
A data breach involving 10,000 CA Consumer PI records where there is a civil suit and AG enforcement action could result in statutory damages ranging between $1,000,000 and $7,500,000 and maximum penalties of $25,000,000 (unintentional) or $75,000,000 (intentional) (and that assumes the AG does not seek penalties of other CCPA violations)
Key CCPA Rights

- Right to know all data collected by a business
- Right to delete your data
- Right to say no (opt-out) to the sale of your information
- Right to be informed of what categories of data will be collected about you prior to its collection and to be informed of any changes to this collection
- Mandated opt-in before sale of children’s information (under the age of 16)
- Right to know the categories of third parties with whom your data is shared
- Right to know the categories of sources of information from whom your data was acquired
- Right to know the business or commercial purpose of collecting your information
- Private right of action when companies breach your data to make sure these companies keep your information safe
Operationalizing the CCPA

— Identify all the ways that a business collects personal information, such as:
  - Directly from consumers
  - By purchase from a third party like a data broker
  - Through analysis of existing data to generate new insights
— Determine whether any transfers to third parties count as “sales” of data
— Figure out what data are subject to CCPA versus what data are exempt
— Update internal privacy policies and external privacy notices with legally required disclosures
— Implement procedures to verify and process consumer rights requests
— Provide appropriate training to personnel
— Implement privacy review procedures to ensure that products, services, and IT systems can support data access, deletion, objection to sale, and other consumer rights requests
— Review and improve security, incident response, and cyber insurance safeguards
Accelerating efforts through GDPR compliance
Poll the audience

— How many of you work for companies with European operations and are subject to the General Data Protection Regulation (GDPR)?

— How many of your companies are leveraging GDPR-built processes for CCPA compliance?

— How many of you performed a GDPR Internal Audit (either before or after May 25, 2018)?
  - Will you leverage lessons learned for CCPA?
## GDPR key facts

<table>
<thead>
<tr>
<th>Category</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Fines</strong></td>
<td>A tiered fining structure depending on infringement. Level 1 is <strong>2% of global turnover</strong> or €10m (whichever is higher). Level 2 is <strong>4% of global turnover</strong> of €20m (whichever is higher).</td>
</tr>
<tr>
<td><strong>Data Protection Officer (DPO)</strong></td>
<td>A DPO required for ‘government bodies’ and organisations conducting <strong>mass surveillance</strong> or <strong>mass</strong> processing of <strong>Special Categories</strong> of data</td>
</tr>
<tr>
<td><strong>Supervisory Authorities (SAs)</strong></td>
<td><strong>Enforcement Powers</strong>  SAs will be given <strong>wide-ranging powers</strong></td>
</tr>
<tr>
<td><strong>Record of processing activities</strong></td>
<td>In general, organizations will need a personal information inventory</td>
</tr>
<tr>
<td><strong>Breach Notification</strong></td>
<td>Requirement to report Privacy breaches to the regulator within 72 hours and potentially to the Data Subject</td>
</tr>
<tr>
<td><strong>Security</strong></td>
<td><strong>Specific requirements</strong> around monitoring, encryption and anonymisation</td>
</tr>
<tr>
<td><strong>Privacy Impact Assessments (PIAs)</strong></td>
<td>Organizations must perform PIAs if the activity is considered ‘high-risk’</td>
</tr>
<tr>
<td><strong>Data Subject’s Rights</strong></td>
<td>Rights extended to include <strong>Data Portability</strong> and the <strong>Right to Erasure</strong></td>
</tr>
<tr>
<td><strong>Sensitive Personal Data</strong></td>
<td>Extended to include <strong>biometric</strong> and <strong>genetic data</strong></td>
</tr>
<tr>
<td><strong>Consent</strong></td>
<td>Requirement to gain <strong>unambiguous</strong> consent (i.e. explicit)</td>
</tr>
<tr>
<td><strong>Data Processors (DP)</strong></td>
<td><strong>Processors</strong> are also covered. Controllers must conduct <strong>due diligence</strong> into processors suitability</td>
</tr>
<tr>
<td><strong>Privacy by Design</strong></td>
<td>Organizations must include the privacy requirements during the development of e.g. new IT Solutions</td>
</tr>
</tbody>
</table>
# GDPR vs. the CCPA

<table>
<thead>
<tr>
<th>Issue</th>
<th>General Data Protection Regulation (GDPR)</th>
<th>California Consumer Privacy Act (CCPA)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Covered Entity</td>
<td>Established in the EU; or NOT established in EU and offering goods and services or monitoring EU Data subjects</td>
<td>Revenues of $25m OR data on 50k residents/households/devices OR 50% of revenue from selling Personal Information</td>
</tr>
<tr>
<td>Enforcement Authority</td>
<td>Supervisory Authority within each EU Member State</td>
<td>California Attorney General</td>
</tr>
<tr>
<td>Scope of Data Subjects/Consumer</td>
<td>Applies to all Data Subjects types including Customers, Prospective Customers, Employees, Suppliers</td>
<td>Applies primarily to Customers and Prospective Customers; limited coverage for HR Data (Applicants, Employees) and B2B (Suppliers) until 2020</td>
</tr>
<tr>
<td>Civil Penalty</td>
<td>Percentage of gross revenues (up to 4%)</td>
<td>Up to $7,500 per violation</td>
</tr>
<tr>
<td>Cure Period</td>
<td>No cure provided</td>
<td>Within 30 days of notification</td>
</tr>
<tr>
<td>Breach Notification timeline</td>
<td>72 hours of becoming aware of breach</td>
<td>Most expedient time possible without undue delay</td>
</tr>
<tr>
<td>Private Rights of Action</td>
<td>EU data subject has right to pursue compensation</td>
<td>Up to $750 per incident or actual damages (whatever is greater)</td>
</tr>
<tr>
<td>Individual Rights</td>
<td>Right of Access, Right to Delete, Right of Data Portability, Right to Rectification, Data Minimization</td>
<td>Do Not Sell My Personal Information, Right of Access, Right to Delete, Right of Data Portability</td>
</tr>
</tbody>
</table>
Internal Audit’s role in privacy compliance
Poll the audience

— How many of you have ever performed an internal audit of your privacy program?
— How many of you have performed an internal audit of your privacy program in the last 12 months?
— How many of you regularly perform internal audits over the privacy program?
Reasons for auditing privacy

— Fulfilling legal obligations (e.g., Regulatory requirement/readiness)
— Fulfilling other obligations (e.g., contractual requirement)
— Requested by supervisory board
— Adhering to sector-specific arrangements (e.g., Code of Conduct)
— Supporting Quality Assurance within organization
— Rebuilding confidence after privacy incidents/breaches
— Controlling sensitive data shared in outsourcing relationships
— Raising further Privacy awareness
Allies of the privacy program

Organizational risk management

— Important allies to any privacy program
— Help privacy functions establish a baseline level of privacy risks and controls
— Risk management mission helps contextualize privacy risk against other organizational risks
— Recurring audits show ongoing efforts to improve the privacy program and help it adapt to changes in organizational risk tolerance and the nature of privacy risk due to business and regulatory changes
— Work with privacy program personnel to define appropriate controls and target maturity levels
Access to senior management and board

**Communicating risk to leadership**

- Raise awareness of privacy risk through observations and findings
- Assurance activities keep board and senior management aware of privacy program implementation progress
- Audits help identify red flags and areas of potential noncompliance
- Independent review of the effectiveness of the privacy program provides objective risk and compliance assurance to the board and management
- Drive change from the top by identifying areas of risk and recommending improvements that leadership can adopt and drive through the business
Accountability and compliance

**Showing organizational accountability**

— Tests of design review documentation against known requirements

— Help privacy program identify what policies and procedures need to be developed or amended

— Tests of effectiveness examine whether the departments, functions and/or processes that the privacy program reviews have effectively implemented documented controls

— Collected evidence can help show reasonable and appropriate practices in case of a regulatory investigation
Accountability and compliance (continued)

Setting up an Audit Plan

— Conduct an initial risk assessment to identify which departments, functions and/or processes should be audited, their relative priority, and audit frequency
— Identify department-specific approaches
— Emphasize communication and coordination among stakeholders
Privacy program maturity

Internal Audit can help a company mature its privacy capabilities to become more value-added and enhancing

Privacy Program Maturity

Privacy isn’t an issue for us... It’s all hype anyway

I have robust policies, processes and controls …

And... a strong second line compliance function

We need a more agile approach to manage the risks

There is no 100% compliance, we need to manage risk

We can’t do this alone – we are part of the community
## Compliance monitoring options

### Level of assurance expected in the industry

1. **Privacy strategy**
2. **Risk appetite**
3. **Risk assessment**
4. **Management testing**
5. **Internal audits**
6. **External audits**
7. **Privacy certification**
8. **Privacy assurance**

### Test strategy (incl. possible key control selection)

- **Test of design**
- **Test of implementation**
- **Test of effectiveness**

### Testing approach

<table>
<thead>
<tr>
<th>Testing approach</th>
<th>Self assessment</th>
<th>Management testing</th>
<th>Internal audits</th>
<th>External audits</th>
<th>Privacy certification</th>
<th>Privacy assurance</th>
</tr>
</thead>
<tbody>
<tr>
<td>Test of design</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Test of implementation</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Test of effectiveness</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>

### Tooling

#### GRC tools

<table>
<thead>
<tr>
<th>DRP</th>
<th>Complions</th>
<th>B-wise</th>
<th>Archer</th>
<th>SAP GRC</th>
</tr>
</thead>
</table>

#### Privacy compliance tools

<table>
<thead>
<tr>
<th>One trust</th>
<th>Nymity</th>
<th>TrustArc</th>
<th>Privacy Perfect</th>
</tr>
</thead>
</table>

#### Specific (privacy) tools

<table>
<thead>
<tr>
<th>Indica</th>
<th>BigID</th>
<th>Dataguise</th>
<th>Evidon</th>
<th>Privaci.Ai</th>
<th>Truyo</th>
<th>SAP access control</th>
<th>WireWheel</th>
</tr>
</thead>
</table>
Auditing CCPA readiness
What to look for with CCPA

— Does your company have proper Governance around CCPA?
  - Sample evidence: X-Functional Team; Program Charter

— Does your company have a plan for CCPA?
  - Sample evidence: Readiness Assessment, Roadmap, Project Plan

— Does your company understand where PI resides and is shared?
  - Sample evidence – Data Inventory, Data Flows
What to look for with CCPA (continued)

— Does your company have the appropriate agreements in place?
  - Sample evidence: Revised Contract Language

— Can your company intake and fulfill Consumer Requests?

— Can your resources verify your customers?
  - Sample evidence: Internal/External verification
What to look for with CCPA (continued)

— Do your company resources have the right training?
  - Sample evidence – Consumer Request Standard Operating Procedures, User Training, General Awareness, Policies

— Does your company have an updated privacy notice?
  - Sample evidence: External Privacy Notice (Website)
Summary

— The privacy regulatory landscape is quickly changing and various privacy laws grant consumers with rights to their data

— The CCPA likely has a significant impact on the way your company does business and interacts with its consumers

— Check the opportunity to leverage GDPR processes to accelerate CCPA readiness for Internal Audit

— Internal Audit definitely has a role in your company’s CCPA readiness and broader program maturity
Questions
Thank you
Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.