Michael A. Gold

Michael is co-chair of the JMBM Cybersecurity and Privacy Group. He counsels clients in a wide variety of matters, including privacy law compliance (including GDPR and the California Consumer Privacy Act of 2018), data breach responses and investigations, crisis management, development of computer-based information retention systems, forensic investigations of computer systems, and computer and internet privacy matters.

Michael also assists clients in developing and implementing information management and governance best practices and developing policies and compliance structures for protecting personal and company information. He was named one of the "Top 20 Cyber – Artificial Intelligence Lawyers" by the Daily Journal (2018), one of the "Most Influential Lawyers: Digital Media and E-Commerce Law" by the Los Angeles Business Journal, and has been designated a "Top Rated Lawyer in Technology Law" by Martindale Hubbell. He is the author of the upcoming Bloomberg BNA portfolio Enterprise Cybersecurity Governance, and co-author of the Bloomberg BNA Portfolio Records Retention for Enterprise Knowledge Management.
What is the CCPA?

- The most comprehensive consumer privacy law enacted to date in the United States

https://www.weforum.org/agenda/2017/12/california-foreign-policy-paradipломacy-la-china/
California Consumer Privacy Act of 2018

What are its salient points?

- **Scope and Effect**
  - Protects “personal information” (PI) of California consumers (i.e., residents)
  - Effective January 1, 2020 — Enforcement starts July 1, 2020
  - Requires compliance with a 12-month “look back” period.

- **Enforcement**
  - Enforced by the California Attorney General (AG).
    - The AG may seek $2,500 per violation for negligent violations, and $7,500 per violation for intentional violations.
  - Private rights of action for consumers if PI compromised as a result of a data breach.
    - Statutory damages in a consumer’s civil suit limited to greater of $100 - $750 per consumer per incident, and actual damages.
What are its salient points? (cont.)

- Disclosure is key
  - Data transfers with vendors and other third parties must be tracked and disclosed.
  - Detailed requirements for privacy policies

- Exemptions
  - Some B2B PI is exempt (expires 1/1/2021).
  - Employee PI is exempt (expires 1/1/2021).
  - De-identified data is exempt in most circumstances.

- AG Regulations
  - The AG issued proposed CCPA regulations that will go into effect on January 1, 2020 – the regulations are extensive, burdensome, and ambiguous.
California Consumer Privacy Act of 2018

Who must comply?

- Annual gross revenue > $25M
- Collects PI for 50,000 consumers annually
- Derives 50% of annual revenue from sale of PI

For Profit entity

Does business in California

Collects personal information from California consumers

Determines purpose and means of processing PI
What is “personal Information” under the Act?

<table>
<thead>
<tr>
<th>Identifiers</th>
<th>Geolocation Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Name, address, email, phone, ssn, license</td>
<td>• GPS coordinates, location history</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Protected Classes</th>
<th>Sensory Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Race, gender, sexual orientation, religion</td>
<td>• Audio, electronic, visual, thermal, olfactory</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Commercial Information</th>
<th>Professional Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Records of personal property, purchasing or consuming histories or tendencies</td>
<td>• Professional and employment-related; CV, employment history</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Biometric Information</th>
<th>Education Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Fingerprints, retina scans, face prints</td>
<td>• Education background, grades, scores</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Internet Activity</th>
<th>Inferences from any of the above</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Browsing history, search history, consumer’s website interactions</td>
<td>• Reflecting preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, aptitudes.</td>
</tr>
</tbody>
</table>
California Consumer Privacy Act of 2018

What “new” rights does the Act confer?

Right of Access
Right to Deletion
Right of Disclosure
Right to Opt-Out (Opt-In for Minors)
Right to Non-Discrimination
What “new” rights does the Act confer? (continued)

- Privacy policy must disclose:
  - What PI is collected?
  - How is it used?
  - With whom is it shared?
  - Is any PI sold?
  - The consumer’s rights and how to exercise them
- Must be updated every 12 months
California Consumer Privacy Act of 2018

The likely impact:

- The Act affects companies worldwide if they collect California consumers’ PI
  - But extraterritorial enforcement is an open issue …
- Other states will adopt similar laws (like Nevada and New York)
  - Federal Government should eventually create a national consumer privacy law
- These laws will cause even more “compliance fatigue.”
- CCPA may spawn significant regulatory enforcement and consumer lawsuits.
And recently…

- Several organizations and Congress have proposed national laws
  - U.S. Chamber of Commerce lobbied Congress for federal legislation that would preempt the CCPA and other similar state laws.
  - The Internet Association and The Interactive Advertising Bureau called for federal laws.
  - None of the proposals have gained any traction yet.

- Alastair Mactaggart, who prompted enactment of the CCPA, has proposed a California ballot measure for 2020
  - If passed, it will restore all of the provisions that were amended out of the Act, add new provisions that will create major obstacles to the sale and transfer of personal information, and will impose crushing burdens on digital advertisers.
What should companies do now?

- Adopt a proactive compliance framework and associated policies that will withstand consumer lawyer and regulatory scrutiny.
- Establish workable protocols and processes to address consumer requests under the Act.
- Determine how to comprehensively and efficiently identify consumer information across all company systems.
- Make sure consumer data is effectively mapped and that the mapping covers the 12-month “look back” period.
- Last but not least - determine who should be in charge.