Defining "Reasonable" Security Under the California Consumer Privacy Act

September 2019

orrick

Introductions

Michelle Visser

Partner

Cyber, Privacy &
Data Innovation

Nicole Gelsomini

Associate

Complex Litigation &
Dispute Resolution

Agenda

- CCPA's Private Right of Action
- Potential Defenses to the Private Right of Action
- Steps to Reduce CCPA Private Right of Action Risk

orrick

California Consumer Privacy Act (CCPA)

- Sweeping new privacy law set to become effective on January 1, 2020.
- Imposes detailed requirements regulating the collection, use, sale, and disclosure of California residents' personal information by qualifying businesses.
- Generally enforced by the California Attorney General, subject to a 30-day cure period.
  - Injunction
  - Civil penalty of $2,500 or (if intentional) $7,500 per violation
- **Key exception**: Creates a private right of action with statutory damages following certain data security breaches.

Private Right of Action – Potential Game Changer

- **Current Environment**: Data breach class actions are frequently (1) dismissed early for lack of actual or likely injury; (2) settled relatively cheaply (frequently well below $1 per consumer in large breaches); or (3) simply not brought.
- **Under the CCPA**: Statutory damages of **$100-$750 per consumer** when certain personal information is subject to an unauthorized access and exfiltration, theft, or disclosure because of a failure to implement and maintain **"reasonable" security measures** - ostensibly even when **no consumer suffers any injury**.

Definition of "Personal Information"

In the private right of action:

An individual's **name**, along with his or her:

- **Social security number**, **driver's license**, or **California identification card number**;
- **account, credit card, or debit card number**, in combination with a **code or password** that would permit access to a financial account; or
- **medical or health insurance** information.

In the rest of the CCPA:

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

Including:

- Protected classifications
- Biometric and geolocation information
- Sensory data
- Internet activity
- Behavioral and profiling data

Potential Defenses – 30-Day Cure

- Before bringing an action for statutory damages, the consumer must give the company written notice of the violation and **30 days to cure** it.
- If the company cures the violation and gives the consumer a **written statement that the violation was cured and that no further violations will occur**, it can avoid statutory damages liability.
- **But** if there is any further violation, the consumer can bring an action for each **breach of the written statement** and any other violation that occurred after the written statement.

Potential Defenses – Due Process Arguments

- "Reasonable" security is not defined in the CCPA - and may be so **vague** as to violate the Due Process Clause.
  - Laws that fail to give fair notice of what conduct is required or prohibited may be void for vagueness.
  - *LabMD, Inc. v. F.T.C.*, 894 F.3d 1221 (11th Cir. 2018):
    - The Eleventh Circuit overturned an order requiring a company to implement a "reasonably designed" security system because the order did not specify what measures would comprise such a system or how reasonableness would be determined.
    - The order's enforcement could have denied the company due process by subjecting it to steep penalties for violating imprecise provisions.

Potential Defenses – Due Process Arguments

- A CCPA statutory damages award may be so **severe and oppressive** as to violate the Due Process Clause.
  - A statutory damages award is unconstitutional when "it is so severe and oppressive as to be wholly disproportioned to the offense and obviously unreasonable." *St. Louis, I.M. & S. Ry. Co. v. Williams*, 251 U.S. 63, 67 (1919).
  - In the TCPA context, defendants have successfully argued that massive statutory damages awards do not comply with due process. *See Golan v. FreeEats.com, Inc.*, 2019 WL 3118582, at *8 (8th Cir. July 16, 2019).
    - But this argument is typically made *after* damages have already been awarded, and would only reduce the award - not eliminate it.

Potential Defenses – Arguing the Security Was "Reasonable"

If Due Process arguments fail, there are several possible ways a court may attempt to measure "reasonable" security, including a **cost-benefit analysis**, **industry custom**, **industry standards**, and/or some combination of these.

But each has its challenges:

- **Cost-benefit analysis**: Are the costs of implementing the security measure outweighed by the potential benefits of implementing that measure (the reduced risk and/or size of a data breach)?
  - *F.T.C. v. Wyndham Worldwide Corp.*, 799 F.3d 236, 255 (3d Cir. 2015) (cost-benefit analysis for FTC Act cybersecurity action).
  - But quantifying the costs and benefits of specific security measures is far from a straightforward exercise.

Potential Defenses – Arguing the Security Was "Reasonable"

- **Industry custom**: Is the security measure ordinarily used in the defendant's industry?
  - *Silverpop Systems, Inc. v. Leading Market Technologies, Inc.*, 641 F. App'x 849, 852 (11th Cir. 2016) (industry custom for negligence cybersecurity claim).
  - *Razuki v. Caliber Home Loans, Inc.*, No. 17CV1718-LAB (WVG), 2018 WL 6018361, at *1 (S.D. Cal. Nov. 15, 2018) (industry custom for California Customer Records Act claim).
  - But there may not be a widely-known industry custom with respect to a particular security measure.
  - And focus on any particular security measure is arguably inappropriate when determining if a company's overall security is "reasonable."

Potential Defenses – Arguing the Security Was "Reasonable"

- **Industry standard**: Is the security measure required by a clearly accepted security framework?
  - Currently, there is no clearly accepted data security standard for all types of personal information subject to the statute.
    - PCI DSS for payment card data.
  - A reasonableness test based on one of the available standards could be dangerous for businesses, particularly if it does not come with a certification safe harbor.

Potential Defenses – Arguing the Security Was "Reasonable"

- A 2016 California AG Data Breach Report stated that the failure to implement relevant **CIS Controls** "constitutes a lack of reasonable security."

Basic

1. Inventory and Control of Hardware Assets
2. Inventory and Control of Software Assets
3. Continuous Vulnerability Management
4. Controlled Use of Administrative Privileges
5. Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers
6. Maintenance, Monitoring and Analysis of Audit Logs

Foundational

7. Email and Web Browser Protections
8. Malware Defenses
9. Limitation and Control of Network Ports, Protocols, and Services
10. Data Recovery Capabilities
11. Secure Configuration for Network Devices, such as Firewalls, Routers and Switches
12. Boundary Defense
13. Data Protection
14. Controlled Access Based on the Need to Know
15. Wireless Access Control
16. Account Monitoring and Control

Organizational

17. Implement a Security Awareness and Training Program
18. Application Software Security
19. Incident Response and Management
20. Penetration Tests and Red Team Exercises

Potential Defenses – Arguing the Security Was "Reasonable"

- Using the CIS Controls as a proxy for reasonableness could be **onerous for companies**.
  - Up to 171 distinct sub-controls, which are not, by their terms, limited in scope.
  - Many sub-controls are open to interpretation.
- Good arguments that the AG Report's statement **should not be entitled any weight**.
  - Released before the CCPA even existed.
  - Not the kind of agency interpretation that receives deference from courts (not a regulation, a rule, an adjudicatory decision, or even an interpretive bulletin).
    - States that it is "for informational purposes and should not be construed as legal advice or as policy of the State of California."

Steps to Minimize CCPA Private Right of Action Risk Now

- **Assess the "reasonableness" of your security**, despite the difficulty of doing so.
  - Seek to comply with emerging standards without suggesting you need to.
    - Potential frameworks:
      - CIS Controls
      - New York DFS Cybersecurity Regulation
      - Massachusetts Privacy Regulation
    - Common themes:
      - Written information security program
      - Governance
      - Ongoing risk assessment and management
        - Table-top exercises
        - Penetration tests
      - Employee training
      - Vendor management
      - An incident response plan

Steps to Minimize CCPA Private Right of Action Risk Now

- Maintain **documentation** of your security practices.
- Preserve **attorney-client privilege** whenever possible over:
  - Pre-incident assessments.
  - Post-incident investigation and assessments.
- Consider **arbitration agreements**.
- Assess opportunities to **shift risk**:
  - Contractual indemnification (e.g., vendors).
  - Cyber insurance.

QUESTIONS?

orrick

Orrick's Privacy Law Webinar Series

- ✓ Want to learn about the new U.S. privacy laws and the impact they may have on your business?
- ✓ Missed a past webinar?
- ✓ Want to attend our next webinar?

California was the first U.S. state to enact a sweeping new privacy law, the CCPA, which comes into effect in January 2020. Nevada has now enacted a scaled-down version of the CCPA that is slated to take effect even sooner – as early as October 2019.

- ✓ Visit **https://www.orrick.com/Cyber-Privacy-Webinars-Videos**

Orrick's Privacy Law Webinar Series
Part #5: Last-Minute CCPA Amendments

Webinar | October 30 | 12pm – 1pm (Eastern Standard Time)

Changes to California's New Privacy Law Ahead of the Effective Date

This webinar is the fifth in a series on U.S. privacy law developments in 2019 and will cover the fate of the CCPA amendments considered this year and what they mean for businesses seeking to finalize their compliance programs.

Presenters

Heather Sussman, Partner
Emily Tabatabai, Partner
Nick Farnsworth, Associate

Orrick's CCPA and GDPR Readiness Assessment Tools

Orrick's ccpa READINESS ASSESSMENT

Test your company against the provisions under the CCPA

- Receive a complimentary report summarizing the likely key impacts
- Use the report to develop your CCPA project plan

Visit: orrick.com/Practices/CCPA-Readiness

Orrick's GDPR Readiness Assessment Tool

Stress test your company against the provisions under the GDPR

- Receive a complimentary report summarizing the likely key impacts
- Use the report to develop your GDPR project plan

Visit: orrick.com/Practices/GDPR-Readiness

Trust Anchor

An established point of trust in a cryptographic system from which a process of validation can begin

Blog: blogs.orrick.com/trustanchor
Twitter: @Trust_Anchor

Michelle Visser

Partner
San Francisco, Boston
T 415 773 5518
E mvisser@orrick.com

Honors

- *Global Data Review* 40 Under 40 (2018)
- *The San Francisco Recorder* Women Leaders in Technology Law (2015)
- *Legal 500* (2015-2019)
- *Law 360* Rising Star (2015)
- *San Francisco Daily Journal* "20 under 40" (2015)
- *Northern California Super Lawyers*, Rising Star (2015)

Education

- Stanford Law School, J.D., 2005, Order of the Coif; Symposium Editor, *Stanford Law Review*; Managing Editor, *Stanford Journal of Law, Business & Finance*
- Calvin College, B.A., Mathematics & Economics, 2002, Honors degree, with greatest distinction

Michelle Visser has extensive experience in defending companies that face the regulatory investigations, class action litigation, and payment card brand claims that frequently follow the announcement of cybersecurity incidents. In addition to litigating privacy and cybersecurity matters, Michelle has navigated numerous companies through their cybersecurity response, including by overseeing technical forensic investigations, advising on notification obligations and coordinating communication strategies.

When faced with an incident, companies call Michelle for crisis response with an eye toward potential litigation. Clients also look to Michelle for privacy and cybersecurity advice before a crisis is at hand. Michelle regularly takes the lessons learned from litigating privacy and cybersecurity matters to provide clients with proactive advice on how to structure their privacy and cybersecurity programs and incident response plans in ways designed to reduce legal exposure.

For her role in representing companies that have faced some of the most high-profile cybersecurity incidents and litigation to date, Michelle was named one of the "40 Under 40" in 2018 by the *Global Data Review* and a "Rising Star" by *Law360* in 2015. She was also recognized as one of the "Women Leaders in Technology Law" by *The San Francisco Recorder* in 2015.

Michelle is also regularly turned to for defense against other types of class actions and complex litigation with experience in defending companies against securities, antitrust, and other commercial claims.

Heather Egan Sussman

Partner
Boston

T 617 880 1830
E hsussman@orrick.com

Honors

- *Chambers USA* (2019)
- *The Legal 500 United States* (2019)
- *Cybersecurity Docket's* "Incident Response 30" (2016, 2018, 2019)
- *Massachusetts Lawyers Weekly* "Top Women of Law" (2015)
- *Best Lawyers* (2018-2019)

Education

- J.D., Boston College Law School, 2000
- B.A., University of Massachusetts Dartmouth, 1996, *magna cum laude*

Heather Egan Sussman is Global Co-chair of Orrick's Cyber, Privacy & Data Innovation practice, and the leader of Orrick's Boston Office. Her practice focuses on privacy, cybersecurity, and information management, and she is ranked by *Chambers USA* and *The Legal 500 United States* as a leader in her field. *Chambers* explains companies turn to Heather because she is "generous with her time and endeavors greatly to educate her clients and understand a given client's risk profile."

Heather's practice focuses on privacy, cybersecurity, and information management. Heather routinely guides clients through the existing patchwork of laws impacting privacy and cybersecurity around the globe. In the United States, this includes advising on federal and state laws such as CCPA, FCRA, ECPA, TCPA, HIPAA, CAN-SPAM, GLBA, state breach-notification laws, and state data-security laws, as well as existing self-regulatory frameworks, including those covering online advertising and payment-card processing. Outside of the United States, she manages teams of talented counsel around the world to deliver seamless advice for clients that operate across many jurisdictional lines, developing comprehensive privacy and cybersecurity programs that address competing regulatory regimes. Heather drafts online privacy notices for global rollout and implements data-transfer mechanisms for the free flow of data worldwide. She helps clients develop and achieve their data innovation strategies, so they can leverage the incredible value of data and digital technologies in ways that not only meet compliance obligations, but also support innovation, deliver value to the business, meet security needs, and solidify brand and consumer trust. Heather helps clients reduce the risk of privacy and security incidents, and in the event of a privacy or security breach, she helps companies respond. She guides clients through comprehensive privacy and cybersecurity assessments worldwide. Heather also regularly counsels businesses on how to mitigate risks associated personal data.

Nicole Gelsomini

Associate
San Francisco
T 415 773 5941
E ngelsomini@orrick.com

Nicole Gelsomini is an associate in Orrick's San Francisco office. Her practice spans cybersecurity and privacy matters, complex commercial disputes, and government and internal investigations.

Nicole has defended companies in class action litigation and government enforcement actions following the announcement of cybersecurity and privacy incidents, as well as the initial investigation of potential incidents. She has also represented clients in securities, antitrust, and other commercial disputes. Prior to law school, Nicole was a teacher and a member of Teach for America's recruitment team.

Education

- Harvard Law School, J.D., 2016, *cum laude*
- University of Colorado, M.A., Education, 2012
- The University of Texas, B.A., Humanities, 2009, *highest honors*