Cybersecurity & Data Breach Response

NELSON MULLINS

Your company's data is one of its most important assets. In the event of a security incident or breach, our team responds immediately:

- Coaching you through the incident
- Advising on each step of the process
- Mitigating the damage and operational disruptions
- Navigating the numerous consumer protection and industry specific notification laws

Ready to respond if a data breach occurs

How we work

- Our team provides individual client attention and 24/7 service
- Our team customizes our approach to meet the needs of individual clients and move efficiently through the life cycle of an incident
- Our team stays ahead of the curve and up to speed as technology and legal requirements change rapidly
- Our team stays focused on swift recovery and damage control aggressively working the case from the first date of discovery to reduce the risk of media, regulatory and litigation fallout

Why Nelson Mullins?

- Highly experienced team
- Available 24 hours a day, every day to respond to a data breach
- Track record of success
- Efficient and organized approach
- Practical solutions when it matters most

We help clients

- Comply with data breach notification requirements by industry and jurisdiction
- Engage forensic experts for assessment, mitigation and ongoing fortification of information technology systems
- Communicate with affected parties, employees, the public, law enforcement and regulators
- Conduct internal investigations and respond to government investigations
- Defend related private and class action lawsuits

Data breaches can impact any business.

We've represented hundreds of clients across industry sectors, including:

- Automotive
- Banking & Financial Services
- Consumer Products & Retail
- Education
- Energy & Utilities
- Health Care
- Hospitality, Leisure & Travel
- Manufacturing
- Real Estate
- Technology
- Transportation

Streamlined process developed from years of experience managing hundreds of security incidents and breaches, including business email compromises, system intrusions and ransomware attacks.

Cybersecurity & Data Privacy Litigation

NELSON MULLINS

In the aftermath of a data incident, experience matters. Our litigators are seasoned trial lawyers who have repeatedly defeated class certification and have tried as lead counsel data privacy class actions to favorable outcomes. When clients need help, our team of experienced litigators can:

- Defend against class actions arising from federal and state privacy laws, including Fair Credit Reporting Act (FCRA), Telephone Consumer Protection Act (TCPA), the Health Insurance Portability and Accountability Act (HIPAA), Family Educational Rights and Privacy Act (FERPA), Electronic Communications Privacy Act (ECPA), and other statutory and common law causes of action for privacy breaches.
- Collaborate to implement a litigation strategy that addresses our clients' business needs and objectives.
- Develop effective strategies to achieve client goals — whether seeking a motion to dismiss, obtaining summary judgment, defeating class certification, or winning at trial.
- Anticipate potential landmines in an environment where data breach class action litigation is increasing and evolving.
- Protect our clients' reputations and manage public relations strategy in high-profile cases.

20+

professionals practicing in cybersecurity and data breach litigation

1,000+ attorneys and professionals

Offices from coast to coast

100+ diversified practice areas

Why Nelson Mullins?

- Extensive trial and appellate experience, including class and collective actions.
- Deep bench including Privacy, Security & Data Breach Response Team.
- In-house e-discovery capabilities to efficiently handle large and complex cases.
- Leveraging technology and software to deliver efficient processes.
- Creative solutions to meet your business goals.

Innovative & robust defense strategies

Our attorneys work collaboratively with clients to strive for desired outcomes from the earliest stages of potential claim development through final resolution of class action and multi-claim litigation.

- **Early responsive action,** including time-sensitive collaboration with data breach response to team to help guide investigations, data preservation strategies, and development of preventive actions to minimize claims and litigation.
- **Regulatory advice and counseling** and responses to regulatory bodies.
- **Exposure and risk assessment** using client data and case experience.
- **Internal and external communications plans** for your board of directors, customers, public agencies, and the public.
- **Case planning and development** oriented to legal defenses, discovery challenges and opportunities, anticipated motions, and ultimate resolution objectives.
- **Litigation plans and budgets** providing strategic methodology and cost containment to "right size" the defense of matters.
- **Class certification challenges** based on both well-established precedents and leading-edge approaches to ascertainability, standing, and commonality of proof in the anticipated trial setting.
- **Shaping the structure and schedules** for multi-claim litigation to meet the needs of the client.
- **Developing corporate and expert witnesses** key to defense and bringing our experience with experts used by opposing parties to the defense.
- **Expert witness** identification and integration into defense.
- **Managing massive ESI productions** by negotiating search terms and efficiencies, protecting privileged materials, and maintaining databases of information for ease of use throughout the litigation.
- **Creating and implementing effective strategies** for evaluating and resolving large inventories of claims cost effectively.
- **Providing billing alternatives** that help clients better maximize corporate certainties regarding the costs of mass litigation.
- **Exploring settlement** in strategic, cost-effective ways and properly documenting and supporting class settlements to withstand scrutiny by courts and attacks by objectors.
- **Trial strategies** that leverage success to reduce exposure.

NELSON MULLINS

June 27, 2024

California AG Continues Privacy Enforcement: Tilting Point Media Settles for Alleged COPPA and CCPA Violations

By Mallory Acheson, CIPM, CIPP/E, Jack Pringle, JD, CIPP/US

In an ongoing effort to enforce the California Consumer Privacy Act (CCPA) and the Children's Online Privacy Protection Act (COPPA), the California Attorney General's Office (CAG) announced a recent settlement against Tilting Point Media, a mobile game publisher. The settlement marks the third public enforcement action under the CCPA and highlights the growing focus and increased nationwide efforts to protect children's online and mobile privacy.

Tilting Point allegedly violated both CCPA and COPPA by collecting and sharing user data, including that of children under 13, without obtaining proper consent. Allegations included:

- Tilting Point's age screen did not ask for a user's age in a neutral way, meaning children were not encouraged to enter their age correctly in order to be directed to a child-version of the game.
- Tilting Point misconfigured third-party software development kits (SDKs), resulting in the collection and sale of kids' data without parental consent.

According to the CAG's announcement, in addition to the payment of a $500,000 fine, Tilting Point must also implement and ensure compliance with the following:

- Not sell or share the personal information of consumers younger than 13 years old without parental consent, and not sell or share the personal information of consumers who are at least 13 but younger than 16 years old without the consumer's affirmative "opt-in" consent.
- In instances where Tilting Point sells or shares the personal information of children, provide a "just-in-time notice" explaining what information is collected, the purpose for collection, if the information will be sold or shared, and a link to the privacy policy explaining the required parental or opt-in consent.
- Use only neutral age screens that encourage children to enter their age accurately.
- Appropriately configure third-party SDKs to comply with legal requirements related to children's data.
- Implement and maintain a SDK governance framework to review the use and configuration of SDKs within its apps.
- Comply with laws and best practices related to advertising to minors and minimize data collection and use from children.
- Implement and maintain a program to assess and monitor its compliance with the judgment, including annual reports.

Continued CCPA Enforcement

Prior to Tilting Point, the CAG secured settlements with:

- **DoorDash** in February 2024 for $375,000 over allegations of mishandling consumer data and failing to provide sufficient CCPA notices and opt-out mechanisms.
- **Sephora** in August 2022 for $1.2 million for allegedly failing to disclose the sale of consumer data and not providing a clear opt-out option, both violations of CCPA.

Key Takeaways

The Tilting Point settlement offers valuable lessons for companies, particularly those dealing with children's data:

- **Prioritize Transparency**: Ensure clear and conspicuous privacy notices that detail data collection practices, use, and sharing.
- **Obtain Verifiable Parental Consent**: Implement a system to obtain verifiable parental consent before collecting any personal information from users under 13.
- **Online Tracking Consent**: implement a system to obtain proper opt-in consent before collecting any personal information from users under 16.
- **Review Third-Party Relationships**: Carefully review data-sharing agreements with third-party vendors, especially those involving user data.

The Tilting Point settlement is just one example of the growing focus on data privacy, particularly when it comes to children. With CCPA enforcement on the rise, and similar laws being enacted across the US and internationally, companies must prioritize data privacy compliance.

Nelson Mullins will continue to monitor state and federal privacy laws and consumer privacy obligations. For more information about CCPA and COPPA or if your business needs assistance with compliance, please contact a member of Nelson Mullins' privacy and cybersecurity practice.

For more information, go to www.nelsonmullins.com.

View on Website

These materials have been prepared for informational purposes only and are not legal advice. This information is not intended to create, and receipt of it does not constitute, an attorney-client relationship. Internet subscribers and online readers should not act upon this information without seeking professional counsel.

GET IN TOUCH

Mallory Acheson, CIPM, CIPP/E

Of Counsel

T 615.664.5378

mallory.acheson@nelsonmullins.com

Jack Pringle, JD, CIPP/US

Partner

T 803.255.9486

jack.pringle@nelsonmullins.com

NELSON MULLINS

June 26, 2024

Next Wave of U.S. State Data Privacy: Effective July 1, 2024

By Mallory Acheson, CIPM, CIPP/E, Daniel C. Lumm, CIPP/US

As of July 1, three new comprehensive state privacy laws – the Florida Digital Bill of Rights (FDBR), the Oregon Consumer Privacy Act (OCPA), and the Texas Data Privacy and Security Act (TDPSA) – will take effect, joining the ranks of existing laws in California, Colorado, Connecticut, Virginia, and Utah.

Here's a quick breakdown of the key aspects of these new laws:

Florida Digital Bill of Rights (FDBR):

This law has a limited scope compared to others and applies to for-profit legal entities doing business in Florida, who collect personal data of Florida residents, control the means of processing, have an annual global revenue exceeding $1 billion, and meet one of the following criteria: (a) derive 50%of its global gross annual revenue from the sale of advertisements online; (b) operate a consumer-smart speaker and voice command service with an integrated virtual assistant connected to a cloud computing service that uses hands-free verbal activation; or (c) operate an app store or digital distribution platform with at least 250,000 different software applications for consumers to download and install.

The FDBR grants consumers rights to access, correct, delete, and opt out of the sale of their personal data and targeted advertising. Additionally, the FDBR includes provisions relating to children's (under 18) data, sensitive data consent, data minimization, annual privacy notice updates, data retention schedules, impact assessments, and prohibitions on government officials moderating content.

While the FDBR doesn't have a private right of action, the Florida Attorney General enforces the law with a discretionary 45-day cure period. FDBR authorizes civil penalties of up to $50,000 per violation and damages may be trebled if an online platform has knowledge that it is violating the rights afforded to children.

Oregon Consumer Privacy Act (OCPA):

The OCPA applies to an individual or legal entity that either: (a) collects personal data from at least 100,000 Oregon residents (excluding data solely for payment transactions); or (b) processes personal data from at least 25,000 Oregon residents and derives more than 25% of their revenue from data sales.

OCPA grants consumers rights to access, obtain, correct, delete, third-party disclosures, and opt out of the sale of their personal data, targeted advertising, and certain profiling. Additionally, the OCPA includes provisions relating to data minimization, children's data, sensitive data consent, opt out preference signals, and data protection assessments. While the OCPA doesn't have a private right of action, the Oregon Attorney General enforces the law that includes a limited cure period of 30 days for violations, ending Jan. 1, 2026. The Oregon Attorney General may seek civil penalties of $7,500 per violation.

Texas Data Privacy and Security Act (TDPSA):

The TDPSA applies to a person or entity who determines the purpose and means of processing personal data and (a) conducts business in Texas by producing products or services consumed by residents of the state; (b) processes or engages in the sale of personal data; and (c) is not a small business, as defined by the U.S. Small Business Administration (unless selling sensitive data).

TDPSA grants consumers rights to access, correct, delete, and opt out of the sale of their personal data and targeted advertising. Additionally, the TDPSA includes provisions relating to data minimization, sensitive data consent, biometric data, and impact assessments.

While the TDPSA doesn't have a private right of action, the Texas Attorney General enforces the law, with a 30-day cure period. The Texas Attorney General may bring an action in court seeking various forms of relief, including declaratory judgment, injunctive relief, civil penalties, attorney fees, and investigative costs. A court may impose civil penalties of up to $7,500 for each violation and if the violation is found to be willful or knowing, treble damages may be awarded.

Nelson Mullins Riley & Scarborough will continue to monitor these state privacy laws and consumer privacy obligations.

For more information about FDBR, OCPA, and TDPSA, or if your business needs assistance with compliance, please contact a member of Nelson Mullins' privacy and cybersecurity practice at www.nelsonmullins.com.

View on Website

NELSON MULLINS

GET IN TOUCH

Mallory Acheson, CIPM, CIPP/E

Of Counsel

T 615.664.5378

mallory.acheson@nelsonmullins.com

Daniel C. Lumm, CIPP/US

Partner

T 864.373.2341

daniel.lumm@nelsonmullins.com