Privacy & Cybersecurity Litigation
Developments, Trends, and Best Practices

Peter Stockburger
Partner
San Diego
619.595.8018
peter.stockburger@dentons.com

Kelly Graf
Managing Associate
Los Angeles
213.892.2811
kelly.graf@dentons.com

Privacy & Cybersecurity Litigation

Roadmap

- **Wiretapping / Plug-Ins / Cookies** litigation developments and trends
- **Data breach** litigation developments and trends
- **TCPA and COPPA** developments and trends
- **State consumer data privacy** developments and trends
- **COVID-19** developments and trends
- Questions

Privacy & Cybersecurity Laws

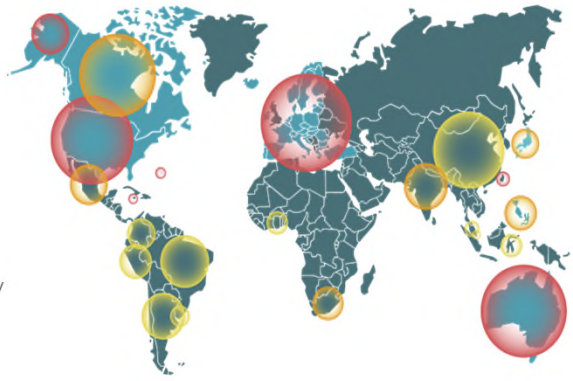
A US Snapshot

Federal			State			
FTC Act	TCPA	GLBA	50 different data breach laws	New consumer privacy laws (CA, NV)	Shine the Light (CA, NY)	Cybersecurity specific (NY, CO)
COPPA	HIPAA	Wiretap Act	Child online safety rules (CA)	Biometric Privacy Laws (IL)	Insurance privacy (CA, CT)	Financial information (CA)

Global Privacy & Cybersecurity Snapshot

Increasing Regulatory Landscape

- EU General Data Protection Regulation (GDPR)
- Canada PIPEDA
- Thailand Data Protection Act
- China Cybersecurity Law
- Vietnam Cybersecurity Law
- Australia Data Protection Law
- Brazil Data Protection Law
- Japan GDPR



Wiretapping / Plug-Ins / Cookies Litigation

Developments & Trends

Key Statutes

- **Federal Wiretap Act** prohibits the unauthorized "interception" of an "electronic communication". (18 USC § 2511)
- **California Invasion of Privacy Act** prohibits using electronic means to "learn the contents or meaning" of any "communication" without consent or in an unauthorized manner. (Cal. Pen. Code § 631)
- **Novel Allegations**: codes embedded on third-party websites (e.g., cookies or related tracking technology) without consent violates law.
- **Defenses**: (1) consent; and (2) "party" to the communication exemption.

Litigation Developments

- **Major tech companies** have been hit with putative class actions.
- **What constitutes adequate consent?** Generally conspicuous and clear, however third-party website arrangement complicates analysis.
- **Circuit split on "party" exemption**. 9th, 1st, & 7th Circuit adopt an industry-unfriendly interpretation. 3rd Circuit uses a more industry-friendly interpretation.
- **What's next** in the litigation battles?

Wiretapping / Plug-Ins / Cookies Litigation

Key Takeaways / Best Practices

- **Data Map**. The only effective way to protect your organization from a novel wiretapping claim is to know what data you collect, where it is stored, which third-parties have access to that data, and how users are informed on those measures.
- **Be Transparent**. Consumers want to know (and in some cases have a legal right to know) what you're doing with their data, and how it will be shared. Avoid generic statements where possible. Transparency can mitigate risk.
- **Be Precise**. Reconsider broad value statements on privacy in public-facing policies and notices. Plaintiffs often use these statements in the lawsuit to draw a contrast against the underlying practices.
- **Review Consent Mechanisms**. As it relates to third-party cookies, this may look like a cookie consent banner, however be careful about a "contract" claim if you require users to agree to the privacy policy in a terms of use. Consider third-party complications.
- **Reconsider Third-Party Relationships**. Not all third-party cookie providers are created equal. Audit your web-presence to determine which providers are necessary, what can be reduced, and how to shore up the disclosures required for each. Data minimization as a best practice.

Data Breach Litigation

Developments & Trends

Statutory Framework

- **50 states**. All 50 states have their own data breach notification statute. Most define "personal information" or "personally identifying information" in a similar fashion, however there are key differences.
- **Federal standards**. Breach notification rules apply under unique regulatory regimes, such as the HIPAA Breach Notification Rule.
- **Contract**. Be wary of notification requirements under contract.
- **Parallel record-keeping laws**. A number of state / federal laws have a parallel statute that require the underlying organization to maintain "reasonable" security around protected information.

Legal Issues and Trends

- **What claims are filed**. Claims often take the form of contract and tort claims, including breach of contract, negligence, failure to notify (under breach statute), and unfair business practices.
- **Article III standing**. Split of federal authority as to whether existence of a breach in and of itself creates an "injury in fact" under Article III. Be wary of providing credit monitoring services (sometimes required), could create standing in some Circuits.
- **Keeping forensic reports out of discovery**. Forensic reports are generally privileged / protected if structured right. Recent decisions throw a wrench into the mix.

Data Breach Litigation

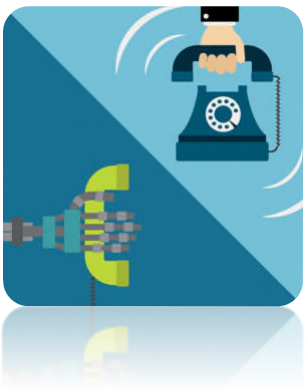
Key Takeaways / Best Practices

- **Map Your Regulatory Obligations**. Understand which state and federal regulatory authority you may be subject to in the event of a security incident, and prepare workflows and incident response planning and management based on those requirements.
- **The Best Offense Is Defense**. Active monitoring of information security program, including legal oversight, is critical in building a defense to a data breach class action.
- **Revisit Incident Response Planning**. An incident response plan is only as good as it is planned and understood by appropriate stakeholders. Plan, manage, and ensure holistic organizational coordination and implementation. In some cases, a robust incident response planning and management program is required by law.
- **Thinking Through Credit Monitoring**. If it's required by statute (e.g., California), OK. If it's not, think through potential impact on standing defenses.
- **Plan Privilege / Work-Product Workflows**. Examine existing contractual relationships, and avoid the "generic MSA" problem. Consider dual-track investigations where appropriate, and ensure participation of legal department early in the incident response planning process.

Telephone Consumer Protection Act (TCPA)

Developments & Trends

- **Scope**. Governs automated telephone calls and text messages (autodialer). Does not cover live calls or messages.
- **High-exposure**. $500-$1,500 per call. 1,000 calls = $1.5m.
- **Litigation explosion**. Cases have been prolific, and expensive.
- **Circuit split**. What is an autodialer?
- **Supreme Court steps into the breach**:
  - ***Barr v. American Association of Political Consultants*** (2020): Upholding sweeping ban of autodialed calls to cellphones, but exception relating to federally backed debts violates 1st Amendment.
  - ***Facebook, Inc., v. Noah Duguid*** (2020): Cert. granted to review what constitutes an "autodialer."



Children's Online Privacy Protection Act

Developments & Trends

- **Scope**. Enacted in 1998. Requires FTC to enforce. COPPA Rule became effective in 2000, and amended in 2013. New amendments being considered.
- **Application**. Applies to operators of commercial websites and online services (apps, IoT) directed to children under 13 that collect, use, or disclose personal information from children, or who direct the collection. Specific rules for disclosure, consent, and review processes.
- **Increased FTC Enforcement**. The FTC has been stepping up enforcement and issuing increasing penalties.
- **Social media and gaming companies** increasingly in the crosshairs.

TCPA / COPPA

Key Takeaways / Best Practices

- **Review your telephone / text message consent regime.** Consent is a defense under the TCPA. How that consent is obtained and manifested, however, varies. Consider where language is placed throughout a website or application, including terms of use and at checkout. Auditing these practices now can save a headache down the road.
- **Align consent mechanisms throughout.** If you are targeting children under 13, or looking to send messages, review how you can align your consent mechanisms under TCPA and COPPA, as well as other privacy regimes such as the GDPR and CCPA.
- **Audit privacy statements.** If you're subject to COPPA, auditing your privacy statements regularly to ensure alignment with the FTC's guidance is critical. For TCPA, review your terms of use.
- **Actively monitor.** The law is quickly changing in both the TCPA and COPPA space. It's crucial your organization have in-house or outside counsel that keeps you abreast of these developments, and how your existing practices may become targeted.

State Consumer Privacy Laws

Developments & Trends

High-Profile State Laws

- **Illinois Biometric Privacy Act (BIPA) (740 ILCS 14 *et seq.*)**. Regulates the collection and use of biometric information. Strict consent regime. Widespread private right of action. Applies outside of Illinois.
- **California Consumer Privacy Act (CCPA) (Cal. Civ. Code § 1798.100, *et seq.*)**. Provides California residents with broad new rights, and imposes strict corresponding obligations on covered businesses. AG enforcement, limited private right of action. Applies outside of California.
- **Unfair business practices / torts**. Often ancillary claims are alleged. CCPA calls into question whether that approach is appropriate.

Litigation Trends

- **BIPA Litigation**. Hundreds of class actions. Illinois Supreme Court held no damage necessary to have standing. Strict compliance requirements.
- **CCPA Litigation**. Limited private right of action for a negligent data breach. What constitutes "reasonable" security? 15 pending class action lawsuits, over 50 referencing the statute.
- **Increase In Related Litigation**. There has been an explosion in lawsuits focusing on claims of breach of contract, negligence, and unfair business practices arising out of these specific statutes. This will only continue to grow.

State Consumer Privacy Laws

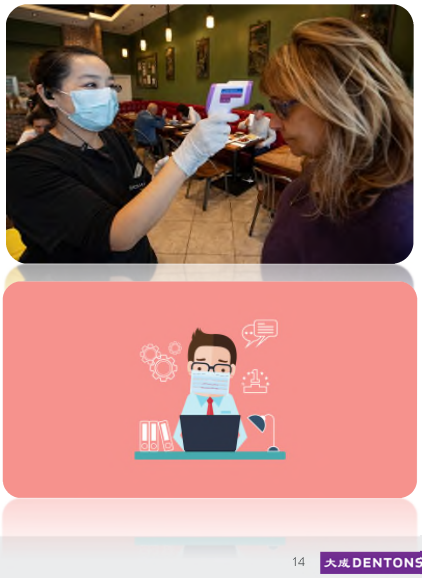
Best Practices

- **Map Your Data**. In order to know whether you are collecting or using data subject to BIPA, CCPA, or other state privacy laws, it is critical to map incoming and outgoing data flows. Both BIPA and CCPA could apply extra-territorially.
- **Audit Privacy Practices**. Both BIPA and CCPA require notice and, in some cases, consent requirements. Prepare new, or audit existing privacy notices and policies to ensure that appropriate language and posture is taken.
- **Biggest risk** for the private right of action is having protected data exposed in a data breach, and there not be reasonable security measures in place.
- **Measure security posture** against, at a minimum, the Center for Internet Security's Critical Security Controls (2016 AG) to determine "reasonable" security requirement. Consider additional frameworks and standards, such as NIST, HITRUST, or other industry standards that may better reflect reasonable security in your particular industry or sector.
- **Ensure California resident personal information is encrypted and/or redacted** at rest or in transit. Review current data sets to see what can be de-identified or aggregated to minimize exposure.
- **Ensure third parties are audited** to protect against flow-down liability.

COVID-19

Privacy Trends

- **Temperature taking** legal issues - federal (ADA / EEOC) and state.
- **Privacy statute exposure** such as the CCPA and related laws
- **Diagnosed** employees…
- **Masks**
- **Working remotely** presents new challenges from a security and privacy perspective.



Questions

Thank you

大成 DENTONS

Dentons US LLP
4655 Executive Drive
Suite 700
San Diego, CA 92121
United States

Dentons US LLP
601 S. Figueroa Street
Suite 2500
Los Angeles, CA 90017
United States

Dentons is the world's largest law firm, delivering quality and value to clients around the globe. Dentons is a leader on the Acritas Global Elite Brand Index, a BTI Client Service 30 Award winner and recognized by prominent business and legal publications for its innovations in client service, including founding Nextlaw Labs and the Nextlaw Global Referral Network. Dentons' polycentric approach and world-class talent challenge the status quo to advance client interests in the communities in which we live and work. www.dentons.com.