ECKERT SEAMANS ATTORNEYS AT LAW

June 28, 2023

Cybersecurity, Data Protection & Privacy Update

New Privacy Civil Litigation Trends in the United States

By Matthew H. Meade, Michael J. O'Brien, and Elizabeth Wilson

Most businesses and institutional non-profits are aware of the litigation risks that arise from a data breach or a violation of specific biometric privacy laws. However, as businesses continue to adopt new technology and/or data sharing practices in their commercial activities, proprietors and leaders should also prepare for consumer lawsuits relating to the dissemination of consumer information without specific authorization, when authorization is legally required.

Companies that use chat features, session replay software, or upload videos on their website are particularly vulnerable to consumer lawsuits in the event they share information derived from such activities with third parties without the consumer's consent. Some state privacy laws provide consumers with a private right of action, but businesses should also prepare for indirect claims filed pursuant to unfair competition laws and/or claims for fraudulent misrepresentation.

As more state legislatures consider the benefits of new data privacy legislation, businesses should monitor legislative developments and recognize future litigation risks. The Table below provides additional information on identified liability risks. In addition, the "In a Nutshell" summary provides an overview of current privacy litigation and discusses what businesses can do to reduce liability.

IN A NUTSHELL

Privacy Litigation Trends

- Companies should be on the lookout for current potential privacy litigation risks going beyond data breach and biometrics lawsuits.
- Privacy lawsuits to watch out for include: (i) claims under the federal Video Privacy Protection Act (VPPA) for the sharing of video watching history, (ii) state wiretapping claims when externally sharing customer chat messages or using online session replay technology, and (iii) state unfair competition or misrepresentation claims arising from violations of new state privacy laws.
- *See the Table below for further information on new privacy litigation trends.*

Who Does This Affect

- *Companies that: (i) use chat and/or video functions on its website or (ii) collect, use, or share personal data in states with state privacy and unfair competition laws.*

What Can You Do Now

- Create and/or update your privacy compliance internal policies and procedures to address potential risks.
- Review and/or update privacy notices to ensure transparency, clarity, and that your data practices are accurately described.
- Where required by law, obtain adequate consent or provide opt out rights to relevant individuals when using or sharing their personal information or communications to you.

- Impose contractual obligations on vendors who collect and use personal data on your behalf to ensure such data and tools are lawfully used when performing services to you.
- Periodically engage with counsel to be informed of new privacy law developments and ensure compliance with newly adopted privacy laws.

Table: Current Privacy Litigation Landscape

Business Activity	***Potential Liability - Video Privacy Protection Act of 1988 (VPPA).***	***How to Reduce Liability***
Automatically sharing a web-user's viewing history of embedded videos on your website with third parties by placing a third-party tracking pixel or other tracking technology on your website.	Many companies have videos on their website with an attached tracking pixel that automatically shares whether an identifiable viewer has viewed the video with a third party such as Meta or YouTube. If the website did not obtain consent from the web-user for such information sharing, the company managing the website may be in violation of a federal privacy law called the Video Privacy Protection Act (VPPA). Individuals can sue the company directly for violations of the VPPA. In 2022, there were 70 VPPA lawsuits filed[1] and courts are currently divided over whether VPPA claims involving use of the Meta pixel is a violation of the VPPA[2].	Check to see if you have any third-party tracking technology that may share website video history with third parties. If you have such tracking technology on your website, make sure that you obtain consent from your web-users before sharing video history or remove the pixel from your website.
Business Activity	***Potential Liability – State Wiretapping Claims***	***How to Reduce Liability***
Sharing the contents of online chat conversations with unauthorized third parties or using third party "session replay" software on your website without consumer consent	All fifty states have some variation of a wiretapping statute which typically prohibits the interception individual communications without consent. Some states, called "all-party" states require the consent of all parties to the communication and violation of the law could trigger a private right of action. Recent litigation has surfaced alleging the interception of online website chat information by third parties. For example, a recent case in Pennsylvania found that a company violated state wiretapping laws by permitting a third-party marketer to "intercept" the consumer's communications with the company on its website.[3] Additionally, the use of third party "session replay" software has also triggered consumer litigation. In April 2023, a class action lawsuit was filed in California against Old Navy[4] for the use of session replay software which monitors and records a web-users' activity on a website (including tracking his/her keystrokes, web-clicks, scrolling activity and webpages visited).	Check which states potential consumer chat users may live and determine whether the state(s) require the consent of all parties to share communications ("all party state"). If your business uses session replay software or records chat conversations from consumers that reside in an "all party state", be sure to obtain consent from the consumer before starting the chat function.

[1] Law.com, *Growing Trend of Data Sharing Litigation: Federal Judge OKs 'Subscriber's' VPPA Suit Against PBS,* March 22, 2023.
[2] JD Supra, *A Recent Surge of Consumer Privacy Litigation Asserting Violations of the Video Privacy Protection Act (VPPA) Seeks to Hold Companies Liable for Data Sharing in Context of Marketing Analytics,* January 26, 2023.
[3] *Popa v. Harriet Carrier Gifts, Inc.*, 52 F.4th 121 (3d Cir. 2022).
[4] *Licea v. Old Navy, LLC*, Case No. 5:22-cv-1413 (C.D. Cal. Apr. 19, 2023).

Business Activity	***Potential Liability - Unfair Competition, Misrepresentation, and Intrusion upon seclusion***	***How to Reduce Liability***
Violating a consumer's privacy rights under state privacy laws to the extent that such violation could fall under a claim of unfair competition, misrepresentation, or an intrusion upon seclusion.	While it is true that existing comprehensive state privacy laws in California[5], Connecticut, Colorado, Iowa, Utah, and Virginia do not have a consumer right to sue for violations of the state law, it is possible that a violation of these laws could be used as evidence to support a state unfair competition or intrusion upon seclusion claim. For example, in the California case *Kellman v. Spokeo, Inc.*[6], the court clarified that the California Consumer Privacy Act (as amended by the California Privacy Rights Act) (CCPA) does not immunize a company's behaviors from liability under California's unfair competition law. More recently, a California judge allowed a class action privacy lawsuit[7] to move forward under the common law theory of intrusion upon seclusion.[8] The Colorado Privacy Act (CPA) expressly notes that a violation of the CPA is considered a deceptive trade practice under the Colorado Consumer Protection Act, which has a private right of action, and may result in an uptick of litigation once the law is in force on July 1, 2023. Likewise, a recently enacted law My Health My Data Act (MHMD) in the State of Washington also provides consumers the right to sue for violations of the MHMD as an "unfair and deceptive" business practice.	Review your existing privacy programs to ensure compliance with state privacy laws. For example, be sure to review your privacy notices to ensure it accurately reflects your company's data collection, use, and sharing practices. Also, ensure your company provides consumers with the ability to opt in and/or opt out of certain data use or sharing activities and make sure to honoring consumer privacy choices and requests to access, delete or correct data. Lastly, if sharing personal data with third parties, ensure your contract imposes adequate data privacy and security obligations on such third parties.

How We Can Help

Eckert Seamans represents publicly traded companies, privately held corporations, nonprofit organizations, small businesses, municipalities, and individuals in complex cybersecurity, data privacy, and related litigation matters.

ECKERT SEAMANS ATTORNEYS AT LAW

This Cybersecurity, Data Protection & Privacy Alert is intended to keep readers current on developments in the law and is not intended to be legal advice. If you have any questions, please contact Matthew H. Meade at 412.566.6983 or https://www.eckertseamans.com/our-people/matthew-h-meade, Michael O'Brien at 215.851.8532 or mobrien@eckertseamans.com, Elizabeth Wilson at 215.851.8497 or ewilson@eckertseamans.com, or any other attorney at Eckert Seamans with whom you have been working for further information and assistance.

[5] Under Section 1798.150 of the California Consumer Privacy Act, individuals have a limited private right of action with respect to certain types of data breaches.
[6] Case No. 3:21-cv-08976-WHO (N.D. Cal. April 19th, 2022).
[7] *Katz-Lacabe v. Oracle America Inc.*, No. 3:22-cv-04792-RS (N.D. Cal. Apr. 6, 2023).
[8] See also a class action lawsuit that was recently filed in California against Tesla for invasion of privacy when Tesla employees would view and share intimate videos of Tesla drivers and their families (including children) while in their home using the car's camera system. *Henry Ye et. al. v. Tesla*, Case No: 3:23-cv-01704 (N.D. Cal. April 7th, 2023).