Litigation Against Healthcare Entities based on their use of Website Cookies and Pixels

By Michael Abraham and Steve Steinberg

The wave of lawsuits against healthcare entities based on the use of website cookies and pixels has continued to accelerate over the past year since we presented on this topic at the May 2023 CSHA Annual Meeting and Spring Seminar. During this same period, new developments in terms of updated guidance from the U.S. Department of Health and Human Services ("HHS"), Office of Civil Rights ("OCR"), a court decision vacating part of OCR's updated guidance, and additional court decisions have shed light on potential defenses against such claims and against class certification. This article covers these developments as well as grounds for pleading challenges and opposing class certification to the commonly pleaded causes of actions. It is important that healthcare entities continue to follow these developments and decisions in order to make informed decisions about the use of analytics and other technologies on their websites, mitigate risk of litigation, and defend against such claims.

Initial Wave of Lawsuits Against Facebook and Healthcare Entities

In 2016, plaintiffs sued Facebook and certain healthcare entities for alleged data sharing through cookies, pixels, and web browser fingerprinting based on the Facebook "share" and "like" buttons on the healthcare entities' publicly accessible webpages. [1] The pleaded causes of action included wiretapping under federal and California law, California Constitutional invasion of privacy and common law intrusion upon seclusion, and negligence per se. The district court dismissed the healthcare defendants based on lack of jurisdiction and dismissed Facebook based on consent arising from the plaintiffs having agreed to Facebook's terms and conditions. The district court decision includes a helpful finding that web browsing data from publicly accessible webpages is not protected health information ("PHI") under HIPAA. The Ninth Circuit in an unpublished memorandum decision upheld the district court, and in so ruling confirmed that the allegedly shared data was not PHI: "Information available on publicly accessible websites stands in stark contrast to the personally identifiable patient records and medical histories protected by these statutes … . Put simply, the connection between a person's browsing history and his or her own state of health is too tenuous to support Plaintiffs' contention that the disclosure requirements of HIPAA … apply." [2]

Then in 2019, plaintiffs filed four cases directly against healthcare entities, alleging similar claims based on a variety of website cookies and pixels, including the Facebook Pixel and Google Analytics. Only one of these actions has been resolved thus far, while two others have passed the class certification stage and continue to be litigated. Specifically, in 2021, Doe v. Partners Healthcare System, Inc., The General Hospital Corp. d/b/a Massachusetts General Hospital, et al., Mass. Super. Ct. for Suffolk County, Case No. 1984CV01651, settled for $18.4 million covering 38 healthcare entity defendants. The settlement class was comprised of all persons who, between May 23, 2016 and July 31, 2021, were patients of any of the defendants, visited any of the covered websites, and were also:

(a) residents of Massachusetts; and/or (b) received medical care in Massachusetts from any of the defendants. Depending on the number of claims, each settlement class member could receive up to $100. In September 2021, a class was certified in Doe v. Virginia Mason Medical Center ("Virginia Mason"), Wash. Super. Ct. for King County, Case No. 19-2-26674-1. And in March 2023, class certification was denied in Doe v. MedStar Health, Inc. ("Medstar"), Maryland Cir. Ct. for Baltimore City, Case No. 24-C-20-000591. Both Virginia Mason and Medstar continue to proceed toward trial.

The Markup Articles and OCR Guidance Trigger a New Wave of Lawsuits Against Healthcare Entities Focused Primarily on the Facebook Pixel

On June 16, 2022, The Markup published an article entitled "Facebook Is Receiving Sensitive Medical Information from Hospital Websites." The article claimed that a significant portion of the top 100 hospitals' websites were using a tracker called the Meta (formerly known as Facebook) Pixel to send data to Meta/Facebook about users' scheduling doctor appointments. Later that year, The Markup published another article entitled "'Out Of Control': Dozens of Telehealth Startups Sent Sensitive Health Information to Big Tech Companies," making similar claims about telehealth companies.

Then, on December 1, 2022, OCR issued guidance on "Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates" that, among other things: [3]

- Defined "tracking technologies" broadly to include "cookies, web beacons or tracking pixels, session replay scripts, and fingerprinting scripts."
- Opined that information collected by a covered entity on its website "generally is PHI, even if the individual does not have an existing relationship with the regulated entity" and even if there is no specific treatment information because it is "indicative that the individual has received or will receive health care services … from the covered entity."

Following the issuance of this guidance, on July 20, 2023, OCR and the Federal Trade Commission issued a letter to over a hundred healthcare systems and telehealth entities reiterating that tracking technologies cannot be used when the shared web browsing data constitutes PHI or confidential information. [4]

The Markup articles and OCR's guidance fueled a new wave of lawsuits that began in 2022 and accelerated in 2023 against healthcare entities based primarily on the Meta (Facebook) Pixel. Most of these cases remain in the pleading motion or discovery stages, though at least four more have led to significant settlements. In May 2023, John v. Froedtert Health, Inc., Wisconsin Circuit Court for Milwaukee County, Case No. 23-CV-1935, related to the Meta Pixel, settled for $2,000,000 with a settlement class of 459,044 consisting of all persons who logged into a patient portal account at least once between February 1, 2017 and May 23, 2022. In August 2023, In Re Advocate Aurora Health Pixel Litigation, E.D. Wisc., Lead Case No. 22-CV-1253-JPS, related to multiple kinds of tracking on the defendant's website, including the Meta Pixel and Google Analytics,

settled for $12.25 million with a settlement class of 2.5 million individuals. More recently, Bustos v. Riverside Medical Center, Cal. Super. Ct. for Riverside County, Case No. CVRI2203466, related to the Meta Pixel, settled for $1,750,000 with an estimated settlement class size of 95,000 consisting of any person who visited the defendant's website at least once between September 9, 2017 and December 13, 2022.The latter is the only known settlement to date of a privacy-related class action concerning website cookies and pixels filed in California. And most recently, Doe v. Lima Memorial Hospital, Court of Common Pleas of Allen County, Ohio, Case No. CV2022 0490, related to the Meta Pixel and other analytics tools on the defendant's website, settled for $1,500,000 with an estimated settlement class size of 211,595 consisting of anyone who was a patient of the defendant and visited its website between January 1, 2018 and May 12, 2023 (motion for preliminary approval pending).

Lawsuit Against HHS and OCR Leads to Revisions in Guidance

On November 3, 2023, the American Hospital Association ("AHA") and others filed a lawsuit against the HHS Secretary, Xavier Becerra, and OCR Director, Melanie Fontes Rainer, over OCR's aforementioned guidance on the use of online tracking technologies. The lawsuit alleged that OCR had inappropriately tried to expand the definition of individually identifiable health information ("IIHI"), that such guidance was preventing healthcare providers from providing information to the public, and that it should have gone through a formal rulemaking process.

On March 18, 2024, OCR issued updated/revised guidance purporting to provide more clarity to regulated entities and the public. [5] Most notably, the updated guidance:

- Acknowledged benefits of "tracking technologies," including to "improve the utility of webpages and apps, or allocate resources."
- Retreated from prior guidance by stating that "[i]n some cases, the information disclosed [through tracking technologies on a regulated entity's website] may meet the definition of individually identifiable health information (IIHI)."
- Acknowledged that "the mere fact that an online tracking technology connects the IP address of a user's device (or other identifying information) with a visit to a webpage addressing specific health conditions or listing health care providers is not a sufficient combination of information to constitute IIHI if the visit to the webpage is not related to an individual's past, present, or future health, health care, or payment for health care."
- Continued to distinguish between tracking on authenticated webpages, which generally requires a visitor to log in and provides access to PHI, and tracking on unauthenticated webpages, which generally does not require login and does not provide access to PHI.
- As to unauthenticated webpages, OCR added that "[v]isits to unauthenticated webpages do not result in a disclosure of PHI to tracking technology vendors if the online tracking technologies on the webpages do not have access to information that relates to any individual's past, present, or future health, health care, or payment for health care."

- OCR provided several new or revised examples of when visits to unauthenticated webpages may or may not involve disclosure of PHI, focusing on the specific intent and purpose of each visit by a person and whether it related to and purportedly revealed the "individual's past, present, or future health, health care, or payment for health care."

However, the examples in OCR's updated guidance did not explain how these distinctions about the visitor's subjective intent in visiting an unauthenticated webpage was to be known by the healthcare entity, including whether the visitor's actions concern their own health or were taken for another reason. [6] Because the visitor's subjective intent for each visit is unknown, on June 20, 2024, the district court presiding over the AHA lawsuit issued a strongly-worded decision vacating the portion of OCR's updated guidance stating that data comprised of a combination of a visitor's IP address and web browsing data from visiting an unauthenticated webpage that addresses specific health conditions (the "Proscribed Combination of Data") could be PHI. [7] The district court held that the Proscribed Combination of Data did not meet the statutory definition of IIHI since: (1) it is unknown if the visit to the webpage was due to the visitor's own health, the health of another person, or for other reasons; and (2) the visitor's subjective intent for the visit is not revealed in such data. [8] As a result, no violation of HIPAA could arise from sharing this combination of data with a third party.

The decision in the AHA lawsuit is consistent with other rulings holding that an agency's guidance is not entitled to deference when it goes beyond the meaning that the statute or regulation can bear. [9] It is also consistent with the Ninth Circuit's previous holding that the connection between data from visits to publicly accessible webpages is too tenuous to be PHI. [10]

The other points in OCR's updated guidance are not vacated by the district court ruling in the AHA lawsuit. OCR reminds covered entities to establish Business Associate Agreements ("BAA") with tracking technology vendors with access to actual PHI. If a vendor will not enter into a BAA, OCR's updated guidance states that a covered entity may establish a BAA with another vendor like a Customer Data Platform that will de-identify the data and disclose only de-identified information to tracking technology vendors. This guidance suggests that the approach of sending actual PHI data to a vendor with a BAA for de-identification prior to sharing it with other third parties may be sufficient for HIPAA compliance from OCR's perspective. We recommend that any such approach be thoroughly vetted before implementation for compliance with HIPAA, and that additional vetting and steps be taken to mitigate the risk of litigation based on other laws, including the California Invasion of Privacy Act's ("CIPA") chapters on wiretapping and pen registers or trap and trace devices. [11]

Potential Pleading Challenges to Claims Based on the Use of Website Cookies and Pixels

- Defenses to Confidentiality of Medical Information Act ("CMIA") Claims

All of the class actions filed in California concerning alleged sharing of data via website cookies and pixels against healthcare entities have originally included claims for violation of CMIA, which, depending on the allegations, can provide for statutory damages of $1,000 per violation. (Cal. Civil Code § 56.36.) However, these claims have proven vulnerable to pleading challenges where, as in many such cases, the plaintiffs cannot plead facts showing actual viewing of medical information by any unauthorized individual. [12]

Additionally, depending on the specific pages where cookies or pixels were allegedly present and the specific information that was allegedly shared, a defendant may be able to argue that web browsing and click data is not "medical information" as defined under CMIA because it does not reveal "substantive" information regarding a person's "medical condition, history, or treatment." [13]

- Defenses to CIPA Wiretap Claims

The class actions filed in California premised on the alleged sharing of data via website cookies and pixels have uniformly included a claim based on CIPA Penal Code § 631(a)'s wiretap provisions, seeking civil penalties of $5,000 per violation under Cal. Penal Code § 637.2. Under applicable case law, a party cannot be liable for wiretapping their own communications. [14] Therefore, to potentially plead a wiretap claim against a healthcare entity that owns a website for its use of cookies and pixels, it involves a combination of the statute's fourth operative clause for purportedly aiding a third party to violate the statute's second operative clause, which prohibits—without the consent of all parties—reading, or attempting to read, or to learn the contents or meaning of any message, report, or communication while the same is in transit or passing over any wire, line, or cable, or is being sent from—or received at—any place within California. This interception requirement has been held to generally not include "obtaining what is to be sent before, or at the moment, it leaves the possession of the proposed sender, or after, or at the moment, it comes into the possession of the intended receiver." [15] While some courts have held allegations of "simultaneous" duplication and transmission are sufficient to defeat a pleading challenge raising the interception requirement, it remains worthwhile to bring such a challenge as cookies and pixels do not involve an interception of data after it leaves the user's device and before it arrives at the intended web server. (There are additional grounds for pleading challenges to a CIPA Penal Code § 631(a) wiretap claim that depend on specific factual allegations and implementations by each healthcare entity, such as the lack of the required content in the data sent to third parties, which are beyond the scope of this article.)

- Defenses to Invasion of Privacy Under California Constitution and Common Law

The class actions filed in California against healthcare entities concerning alleged sharing of data via website cookies and pixels have typically included claims for invasion of privacy under the California Constitution and/or intrusion upon seclusion under the common law. These have sometimes survived pleading challenges. However, pleading challenges can be made based on the arguments that: (1) there is no reasonable expectation of privacy in web browsing data from publicly accessible webpages because they contain general information that is not specific to any individual nor, as set forth in the decision from the AHA lawsuit, is the visitor's subjective intent for the visit revealed in the data; [16] and (2) using Internet cookies on and sharing web browsing data from such webpages is not "sufficiently serious" or "highly offensive." [17]

- Consent Defense Against All Claims

Depending on the pleaded or judicially noticeable facts, pleading challenges based on the defense of consent can defeat a CIPA wiretap claim as well as other statutory, Constitutional, and common law claims. For example, if the visitor has consented to the sharing of data by their actions—such as by clicking to allow cookies on a cookie banner, or by continuing to use the website with the knowledge that sharing of data is taking place, or by having entered into an enforceable agreement—by clicking to create an account—that authorized the sharing of data, no wiretap claim, common law tort claim, Constitutional privacy claim, or contract claim should exist. [18]

Potential Defenses Against Class Certification

Because of the potential for substantial statutory damages and civil penalties in cases against healthcare entities premised on the use of website cookies and pixels, class certification represents a major inflection point. Only two such healthcare cases—Virginia Mason and Medstar—have concluded the class certification stage, and as noted above, class certification was granted in Virginia Mason and denied in Medstar.

A party seeking class certification in California must demonstrate: "[1] the existence of an ascertainable and sufficiently numerous class, [2] a well-defined community of interest, and [3] substantial benefits from certification that render proceeding as a class superior to the alternatives." [19] To show a "well-defined community of interest" depends on: "(1) predominant common questions of law or fact; (2) class representatives with claims or defenses typical of the class; and (3) class representatives who can adequately represent the class." [20] A class action cannot be used where each member would be required to individually litigate numerous and substantial questions. [21] Further, a class action cannot be used if it would abridge the defendant's right to present unique defenses or would be unmanageable. [22] In the context of cases based on sharing of data from the use of cookies and pixels, strong arguments against class certification exist.

Most notably, whether and what data was sent to, received, and/or viewed by a third party for each visit to a website is far from uniform. Rather, individualized assessment is needed concerning the web browser's configuration, including cookie settings, and whether and what browser plugins or extensions were installed, as well as what webpages were visited and what actions were taken. For example, the visitor's browser settings may have blocked potential transmission of data to a third party in whole or part. Alternatively, the visitor's settings may have prevented such data from being associated with the visitor. Likewise, the visitor may have used plugins or extensions to prevent sharing of data. Class certification has been denied on this basis. [23]

Further, what cookies and pixels were present on a particular webpage, or what cookies were stored in the visitor's browser due to their independent actions, (such as whether a Facebook user cookie was present on the visitor's device due to the visitor having recently logged into their Facebook account, or whether they were logged into a Google Gmail account), can and often does vary over time. Similarly, what particular action on a webpage was needed to trigger particular cookies or pixels can vary over time. These variations have significant impacts. As a result, individual assessment is needed, including so the defendant can present unique defenses as to each putative class member and each visit, thereby resulting in individualized issues predominating as well as a lack of the required manageability. [24]

In addition, the method of access used for each visit may preclude liability. Many healthcare systems and providers allow patients to log into a portal through a mobile application. In most cases, the mobile application does not involve the use of cookies or pixels, even if the website does. As a result, to the extent a particular visitor used the mobile application and depending on the actions taken during the visit, there may be no potential for data having been shared with any third party due to cookies and pixels. Thus, assessment of each visit is required, thereby making individualized issues predominate and proceeding by class action unmanageable.

An argument also exists that Penal Code § 631's wiretapping provisions are limited to interception of transmissions over wired landlines as distinct from wireless transmissions. [25] Whether a particular visit was done by means of a wired landline cannot be determined in each case from the defendant's web server logs. If this argument is upheld, individualized issues predominate and/or proceeding by class action is unmanageable because individual assessment via cross-examination or written discovery is needed to determine whether the particular visit was done using wired landlines versus wireless means. [26]

Individualized issues also predominate, and the required manageability is also absent, with regard to each putative class member's consent. Class certification has been denied and upheld on appeal based on the defendant having the due process right to litigate the issue of consent as to each putative class member. [27]

Conclusion

The above discussion addresses OCR's updated guidance to healthcare providers as modified by the recent district court decision in the AHA lawsuit, as well as grounds for challenging the pleadings, and opposing class certification, as to commonly asserted causes of action. Additional grounds for pleading challenges and opposing class certification exist depending on the specific facts, causes of action, and/or website's operations. The case law in this area continues to rapidly develop, with new decisions being issued on a monthly basis. These developments have reaffirmed that strategies exist not only for defeating these lawsuits, but also for lowering the risk of being subjected to such a lawsuit while at the same time obtaining the benefits of analytics.

Endnotes

[1] Smith v. Facebook, Inc., (N.D. Cal. 2017) 262 F.Supp.3d 943.

[2] Smith v. Facebook, Inc., (9th Cir. 2018) 745 Fed. Appx. 8.

[3] https://web.archive.org/web/20221201192812/https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html.

[4] https://www.ftc.gov/system/files/ftc_gov/pdf/FTC-OCR-Letter-Third-Party-Trackers-07-20-2023.pdf.

[5] https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html.

[6] See Smith, 745 Fed. App'x 8 ("... the connection between a person's browsing history [on publicly accessible websites] and his or her own state of health is too tenuous to support Plaintiffs' contention that the disclosure requirements of HIPAA ...apply.").

[7] American Hospital Association v. Becerra, _ F.Supp.3d _ (2024), 2024 WL 3075865

[8] 42 U.S.C. § 1320d(6): (1) "relates to" an individual's "past, present, or future physical or mental health or condition," the individual's receipt of "health care," or the individual's "payment for" healthcare; and (2) "identifies the individual" or provides "a reasonable basis to believe that the information can be used to identify the individual."

[9] California v. U.S. Dep't of Health & Hum. Servs., (9th Cir. 2019) 941 F.3d 410, 425 ("an agency's interpretation of a statute is not entitled to deference when it goes beyond the meaning that the statute can bear"); Kurowski v. Rush Sys. for Health, (N.D. Ill. July 24, 2023) No. 22 C 5380, 2023 WL 4707184, at *4 ("The interpretation of IIHI offered by HHS in its guidance goes well beyond the meaning of what the statute can bear." [addressing OCR's original guidance]; and holding the metadata was not IIHI.]).

[10] See footnote vi, supra.

[11] Cal. Penal Code, §§ 631, 638.51.

[12] See Sutter Health v. Super. Ct. (Atkins), (2014) 227 Cal.App.4th 1546 (writ issued directing demurrer be sustained without leave to amend); B.K. v. Eisenhower Med. Ctr., (C.D. Cal. Feb. 29, 2024) No. EDCV 23-2092 JGB (KKx), 2024 WL 878100, at *4 (dismissing CMIA claim based on Meta Pixel for failure to allege facts showing improper viewing]; but see Doe v. Regents of Univ. of California ("Regents of U.C."), (N.D. Cal. 2023) 672 F.Supp.3d 813, 819 (denying motion to dismiss CMIA claim where plaintiff allegedly received tailored ads and targeted emails based on heart and blood pressure issues only after entering such information in the patient portal).

[13] Eisenhower Med. Ctr. v. Super. Ct., (2014) 226 Cal.App.4th 430, 435-37; Cal. Civ. Code § 56.05(j); see also B.K., 2024 WL 878100, at *4 (dismissing CMIA claim for lack of specificity about allegedly disclosed "medical information"); but see Regents of U.C., 672 F.Supp.3d at 819 (denying dismissal); B.K. v. Desert Care Network, (C.D. Cal. Feb. 1, 2024) No. 2:23-cv-05021 SPG (PDx), 2024 WL 1343305, at *5 (denying motion to dismiss CMIA claim based on Meta Pixel allegedly transferring data on use of patient portals to schedule appointments, refill prescriptions, and view test results and appointment notes).

[14] Rogers v. Ulrich, (1975) 52 Cal.App.3d 894, 899.

[15] People v. Malotte, (1956) 46 Cal.2d 59, 64 & n. 1.

[16] See Smith, 262 F.Supp.3d at 954-55, aff'd 745 Fed. App'x 8 (holding that shared data from publicly accessible webpages is not PHI).

[17] See Low v. LinkedIn Corp., (N.D. Cal. 2012) 900 F.Supp.2d 1010, 1024-26 (dismissing invasion of privacy claims based on use of cookies on these grounds); In re Nickelodeon Consumer Privacy Litig., (3d Cir. 2016) 827 F.3d 262, 294-95 (dismissing intrusion on seclusion claim against Google based on holding that "tracking cookies can serve legitimate commercial purposes" and the use of "cookies on websites geared toward adults" is generally acceptable); but see In re Meta Healthcare Pixel Litig., (N.D. Cal. Jan. 29, 2024) No. 22-CV-03580-WHO, 2024 WL 333883, at **1-3 (denying motion to dismiss constitutional privacy and intrusion on seclusion claims based on use of Meta Pixel).

[18] See Smith, 262 F.Supp.3d at 947, 949-50, 953-56 (consent precluded claims asserting wiretap, constitutional and common law invasion of privacy, negligence per se, and breach of duty of good faith and fair dealing); Smith, 745 Fed. Appx. 8 (same); see also Long v. Provide Commerce, Inc., (2016) 245 Cal.App.4th 85(discussing when an online agreement is enforceable].

[19] Brinker Restaurant Corp. v. Super. Ct. (Hohnbaum), (2012) 53 Cal.4th 1004, 1021.

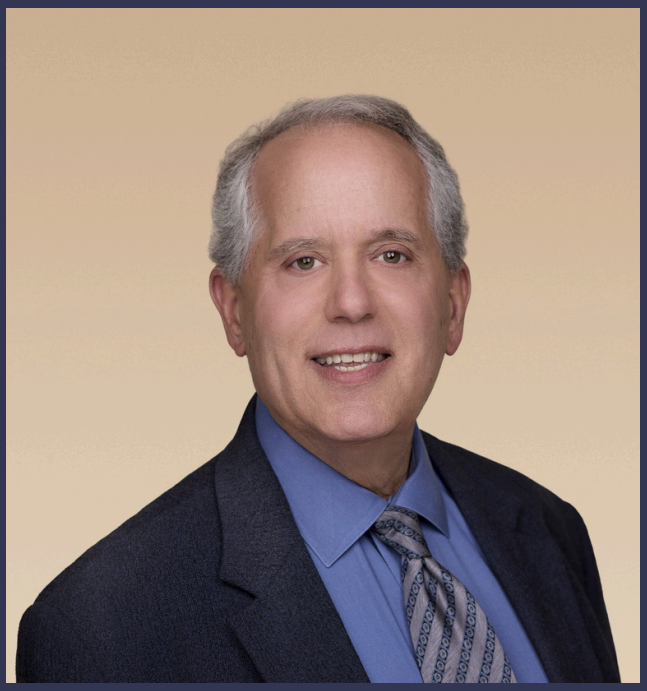
[20] Id. [quotations omitted].

[21] Wash. Mutual Bank, FA v. Super. Ct., (2001) 24 Cal.4th 906, 913–14.

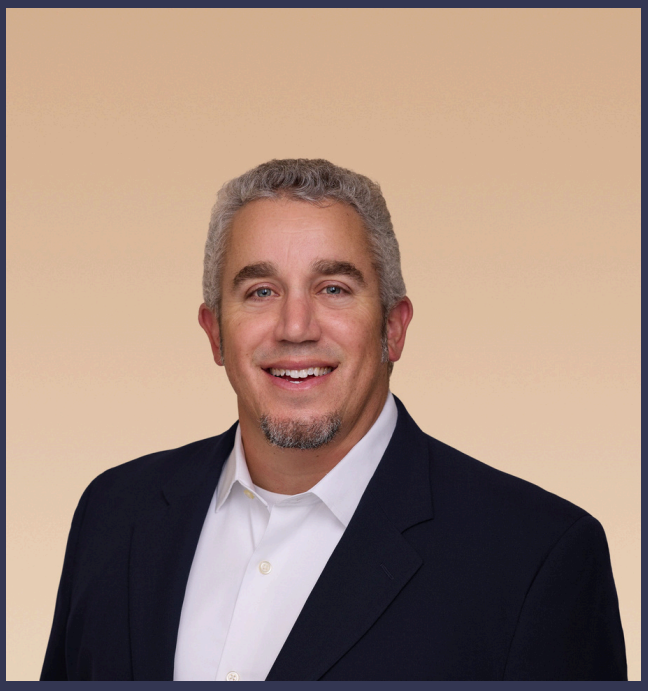
[22] Duran v. U.S. Bank Nat'l Assn., (2014) 59 Cal.4th 1, 30.

[23] See In re Hulu Privacy Litig., (N.D. Cal., June 17, 2014) No. C 11–03764 LB, 2014 WL 2758598, **21-22 (denying class certification because browser configurations that blocked sharing of data or caused clearing of cookies made individualized issues predominate).

[24] Duran, 59 Cal.4th at 30 (class action cannot abridge the defendant's due process right to present unique defenses nor be used where it would be unmanageable); Hataishi v. First Am. Home Buyers Prot. Corp., (2014) 223 Cal.App.4th 1454, 1466-68 (denial of class certification upheld; due process required the defendant be allowed to cross-examine each individual as to their unique circumstances).
[25] Tavernetti v. Super. Ct., (1978) 22 Cal.3d 187, 190 (Penal Code § 631(a) prohibits interception of wire communications).
[26] Hataishi, 223 Cal.App.4th at 1457-60, 1463-68 (upholding denial of class certification in a Penal Code § 632 eavesdropping case and denial of leave to amend to add a different CIPA section because it still would require individualized assessment to determine if wired versus wireless means were used for each visit).
[27] See Kight v. CashCall, Inc., (2014) 231 Cal.App.4th 112, 132 (upholding denial of class certification in a CIPA Penal Code § 632 eavesdropping case because "the defendant has the right to litigate the issue of each class member's consent"); see also Penal Code § 631 (wiretapping provisions have the same "without the consent of all parties" requirement found in § 632).



Michael Abraham is a partner in the Bartko LLP law firm. He has over 35 years of litigation experience. His healthcare practice focuses on representing healthcare systems, entities, and providers with respect to litigation involving privacy, website analytics, peer review proceedings, antitrust issues, and commercial disputes. On behalf of healthcare entities, technology companies, Department of Defense contractors, and other clients, Michael has successfully handled a wide range of litigation as well as government investigations. He is an update author for the CEB treatise on Privacy Compliance and Litigation. Michael can be reached at 415-956-1900 or mabraham@bartkolaw.com.



Steve Steinberg is a partner in the Bartko LLP law firm. He has 20 years of trial and litigation experience focused on privacy, intellectual property, cryptocurrency, CIPA claims over alleged wiretapping, pen registers and trap and trace devices, and other complex business disputes. He has defended healthcare systems, entities, and providers in actions involving wiretap and privacy claims based on website cookies and pixels, civil rights claims, breach of contract, and a wide variety of other claims. Steve is an update author for the CEB treatise on Privacy Compliance and Litigation. Steve can be reached 415-956-1900 and ssteinberg@bartkolaw.com.

Michael and Steve, along with other members of the Bartko law firm, are actively defending multiple class actions involving claims based on website cookies and pixels on behalf of major healthcare systems and other entities. They have had substantial success in defeating claims at the pleading and preliminary injunctive stage, limiting discovery, and opposing class certification. Additionally, at the trial and appellate levels, they had key roles in establishing leading decisions concerning the California Confidentiality of Medical Information Act.