Two New Waves of Privacy Class Actions May Affect Financial Institutions

Related Professionals

Marcel C. Duhamel

Related Services

Corporate and Business Organizations

Related Industries

Financial Institutions

AUTHORED ARTICLE | Fall 2023

By Marcel Duhamel
(Published in the Fall 2023 issue of *The Bankers' Statement*)

A number of privacy class actions have been filed in federal courts, and in California state courts, that may have an impact on financial institutions. One wave of these cases challenges the use of Meta's Pixel technology, and the other challenges the use of third-party providers of chat or "session replay" services. Both rely on federal or state wiretapping theories, and some seek to hold the operators of websites liable on an "aiding and abetting" theory. While these cases—so far—have not targeted financial institutions, there is no reason to believe that banks and consumer lenders using these technologies will not join the ranks of defendants.

Meta Pixel Cases

The first line of cases—perhaps only the tip of the spear—is represented by *Doe v. Regents of the University of California*, currently pending in the United States District Court for the Northern District of California. The plaintiff—on behalf of a putative class—alleged that University of California San Francisco Medical Center (UCSF) installed Meta's Pixel tool on its website and on an online patient portal. As the complaint describes it: "Meta Pixel is a snippet of code that, when embedded on a third-party website, tracks a user's activity as the user navigates the website. As soon as a user takes any action on a webpage that includes the Meta Pixel, the code embedded in the page re-directs the content of the user's communication to Meta while the exchange of the communication between the user and website provider is still occurring." Thus, "the Meta Pixel intercepts the pages a user visits, the buttons they click, and some information they input or search and transmits that information, along with the user's IP address, to Meta." The complaint alleges that "Meta then uses this information to provide targeted advertisements to the Facebook user and to train its algorithms to more accurately identify and target users."

The plaintiff alleged several theories: (1) violation of the California Invasion of Privacy Act (CIPA), which is quite similar to the federal Electronic Communications Privacy Act (ECPA), which updated the Federal Wiretap Act; (2) violation of the California Confidentiality of Medical Information Act (CMIA); (3) a privacy claim under the California constitution; and (4) a common law breach of privacy claim. The court dismissed the CIPA claim, but on grounds that would not be applicable to financial institutions: the CIPA does not apply to public entities. It dismissed the constitutional claim because the plaintiff sought damages. It allowed the CMIA claim and the common-law breach of privacy claim, however, to proceed.

The court did not reach the question whether the defendant could have been liable under CIPA were it not a public entity. A concern for financial institutions may be that a claim under CIPA (or the federal ECPA) might survive a motion to dismiss, and even if not, a claim for violation of financial privacy statutes might be seen as analogous to the claim for breach of medical privacy. Financial institutions, in other words, could face similar claims if they install Meta Pixel on financial information portals. Even if not, if they install Meta Pixel on websites generally, that could give rise to a claim on a common law breach of privacy theory.

Chat Services Cases

The second line of cases involves a website owner's incorporation of on-line chatbots, an increasingly common tool used to allow a website visitor to "chat" with a "virtual" customer service representative. Often, allegedly unbeknownst to the consumer, the chatbot is hosted by a third-party provider, and the chats are sent to and by that provider and stored on the provider's servers. Class action lawyers have, in the last 24 months, filed scores of putative class actions alleging, generally, that the third-party server is engaged in wiretapping and that the website owner is aiding and abetting that wiretapping.

Two cases are particularly representative, in that they involve the same named plaintiff represented by the same counsel, were filed in the same jurisdiction, and have had different outcomes on motions to dismiss. The first is *Byars v. Hot Topic, Inc.*, 2023 U.S. Dist. LEXIS 24985 (C.D. Cal. Feb. 14, 2023). There, the plaintiff alleged that the defendant's use of a third party chat service, without disclosure to the plaintiff, violates the California Penal Code, which provides in relevant part:

> (a) Any person [1] who, by means of any machine, instrument, or contrivance, or in any other manner, intentionally taps, or makes any unauthorized connection, whether physically, electrically, acoustically, inductively, or otherwise, with any telegraph or telephone wire, line, cable, or instrument, including the wire, line, cable, [*21] or instrument of any internal telephonic communication system, or [2] who willfully and without the consent of all parties to the communication, or in any unauthorized manner, reads, or attempts 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 this state; or [3] who uses, or attempts to use, in any manner, or for any purpose, or to communicate in any way, any information so obtained, or [4] who aids, agrees with, employs, or conspires with any person or persons to unlawfully do, or permit, or cause to be done any of the acts or things mentioned above in this section. . . . [is liable].

Cal. Penal Code § 631. After noting that the plaintiff and her counsel had filed "at least 58 of these virtually identical lawsuits" and that they all appeared to be essentially identical except for an introductory paragraph, the court concluded that a business cannot eavesdrop on its own communications. Relying on earlier rulings in a similar case, the court held that "the facts as pled show that [the third party] acted as a

recorder, and not as an eavesdropper." The court's conclusion appears to have been driven by the plaintiff's failure to plead that the third party used the recorded data for its own purposes; the third party was not alleged to be engaged in the "aggregation of data for resale," but instead appeared, from the facts as pled, to act as "an 'extension' of the defendant's website."

The plaintiff also alleged a violation of Cal. Penal Code § 632.7, which provides in relevant part:

> Every person who, without the consent of all the parties to a communication, intercepts or receives and intentionally records, or assists in the interception or reception and intentional recordation of, a communication transmitted between two cellular radio telephones, a cellular radio telephone and a landline telephone, two cordless telephones, a cordless telephone and a landline telephone, or a cordless telephone and a cellular radio telephone [is liable]

The court held: "The unambiguous meaning of the statute is thus that it only applies to communications involving two telephones. Plaintiff's allegations all relate to text-based web communications regarding a chat feature on a website, which virtually by definition cannot involve two telephones." Consequently, the court dismissed this count, concluding that "whoever or whatever is on the other end of the text-based communication, a computer, and not a telephone, is being used to send a receive messages to Plaintiff and other users of the Website."

In stark contrast is another case involving the same named plaintiff, represented by the same lawyer, making identical claims, but before a different judge: *Byars v. Tire*, 2023 U.S. Dist. LEXIS 22337 (C.D. Cal. Feb. 3, 2023). There, in a decision entered 11 days prior to the Hot Topic decision, another judge in the same district declined to dismiss plaintiff's complaint. Analyzing the §631(a) claim, the court made short work of holding that plaintiff had adequately alleged that defendant "intercepted" her communications "using a third party service." The court did not address any argument that the third party service was acting on the defendant's behalf, as did the Hot Topic court.

Similarly, the court refused to dismiss the claim under §632.7. There, the court brushed aside arguments that the plaintiff had failed to allege that the communications involved two telephones: "there is no requirement that Byars allege the type of telephonic device used by" the defendant. The court did not directly address the distinction between alleging the ***specific type*** of telephonic device on the one hand and alleging ***the use of any telephonic device*** in the first place.

Whatever one thinks of the competing rulings, one thing is clear: in at least some courts, "wiretapping" claims, whether pled under California law or analogous federal or state law, may survive motions to dismiss. This is consequential: in most circumstances, class certification is decided prior to summary judgment. If a putative class case survives a motion to dismiss, at a minimum the defendant will be forced to endure class discovery and the substantial legal fees associated with class certification proceedings. In the event a class is certified, the possibility that the defendant might prevail on a summary judgment motion after failing to win a motion to dismiss might be small comfort; substantial expenses will have been incurred by that point, and the risk of an adverse result will sometimes drive defendants to pay large settlements even when their defenses may appear strong.

Takeaways

Legal teams at financial institutions should understand whether their marketing and customer service teams are deploying third-party services to track web page interactions and customer service interactions. If they are, the legal team should assess whether the benefits of using these services justify the risk of exposure to class claims alleging that allowing these third parties to have access to customer web page behavior or customer service "chats" violates their customers' reasonable expectations of privacy. They should also carefully review disclosures made to customers and assess whether the use of these services is fully and clearly disclosed, and should consider whether customers should be required to "opt-in" or otherwise affirmatively consent to the use of these technologies.

Even meritless claims presented as class actions can generate considerable risk and large legal fees. Financial institutions should deploy these technologies—if at all—with a clear-eyed view of these risks. If they chose to accept the risk, they should carefully review whether they provide fair notice and consider whether to offer customers the choice of whether their data will be shared with these service providers. In some jurisdictions, providing that choice may be mandatory under some circumstances.

While banks have not yet been the focus of these claims, nothing suggests that financial institutions will not eventually join the growing ranks of defendants.