

Healthcare Provider Beware: Massachusetts Federal Court Largely Permits Tracking Technologies and Wiretapping Claims To Proceed

Article By:

Scott T. Lashway

Matthew MK Stein

In the privacy world, pixels, cookies, and tracking technologies get all the attention these days. Plaintiffs and regulators alike have been working to persuade courts nationwide that the presence of third-party tracking software on a website can be an infringement of website visitors' privacy rights, as if the open highways of the Internet bestow some "promise" of anonymity upon website users such as an absolute right to privacy in their interactions with a website. This has become particularly poignant for healthcare companies (of varying stripes) who face a plaintiff's bar bent on using the HIPAA Privacy and Security Rules against providers and plans alike, even though HIPAA *still* does not have a private right of action.

Last month, in [*Doe v. Tenet Healthcare Corporation*](#), a widely respected jurist sitting on the federal court in Boston largely upheld privacy claims under Massachusetts law against a hospital over its use of an often-used social media pixel and other tracking technologies on its website. **The single most important takeaway is beware: the court's allowance at the motion to dismiss stage of various claims to proceed represents the seriousness of these matters, and the credibility with which the court regarded the plaintiff's allegations is concerning.**

In its ruling, the court upheld claims under Massachusetts law for negligence, breach of fiduciary duty, breach of implied contract, unjust enrichment, and violations of the Massachusetts Right to Privacy law, chapter 93A, and Massachusetts wiretap law:

1. **Breach of fiduciary duty:** To the court, a fiduciary relationship exists between a provider and patient, and therefore because the plaintiff alleged she was a patient of the hospital, she sufficiently pled that the hospital breached its fiduciary duties to her by using the pixels and other tracking technologies to disclose her confidential information. The SJC has held that **physicians** owe a fiduciary duty to their patients, and some Superior Court decisions have extended that to pharmacists (and pharmacies); but this decision represents an ipse dixit expansion of the rule to hospitals for information provided to the hospital in connection with scheduling care, identifying physicians, or accessing the patient portal. This is a very noteworthy analysis by the court; one that will be challenged under standing Massachusetts

law.

2. **Negligence:** Because the court found a fiduciary duty, the court concluded plaintiff's negligence claim was not barred by the economic loss doctrine. Moreover, the court viewed the plaintiff's allegations that the tracking technologies were a proximate cause of the hospital's alleged disclosure of her information to third parties, which used the information to direct targeted advertising to the plaintiff about her medical condition. Finally, to the court, the plaintiff alleged damages because she did not consent to the disclosure to the tracking technology providers, even though she typed the information allegedly shared into public pages of a public website, further erasing the line between expectations of privacy and expectations of anonymity as a form of privacy.
3. **Breach of implied contract:** The court fashions an implied contract from the hospital's privacy policies, both its online/website privacy statement and its HIPAA-mandated Notice of Privacy Practices, and a patient's "reasonable expectation under HIPAA, as well as the privacy policies," that information entered into the hospital's website will be kept private and not sold to third-party companies. It may have been important to the court that the hospital's Notice of Privacy Practices "promise[d]" the plaintiff needed to provide written information before her information would be sold or disclosed to third parties and did not distinguish between where information was collected by the hospital, online or offline, in public or in the privacy of a treatment room. Arguably this could mean that if a patient yelled health information across a crowded field to their doctor, the doctor alone could not disclose it, even though every other person on the field who heard the information could and the patient could not reasonably have expected any privacy for that information. That would be an absurd result, and yet is plausible under the court's apparent reasoning.
4. **Unjust enrichment:** To the court, the plaintiff's allegation that her private information had marketing value to third parties and that she paid for medical services in the expectation that the hospital would not disclose her private information was sufficient to state a claim for unjust enrichment. Left unsaid is that the "private information" had marketing value to the hospital (or indeed, that the hospital used the information for marketing purposes), and yet the court decided the plaintiff alleged that the hospital retained a benefit and that retaining that benefit was unjust. If nothing else, this raises the question of what part of the treatment costs were for keeping the information confidential. Surely not all: the hospital is entitled to a reasonable benefit it can keep in exchange for providing the plaintiff with medical care. This also raises the question of whether any of the information at issue in the complaint has any connection at all with the care treatment received.
5. **Massachusetts Right to Privacy Law:** On this claim, the court follows prior decisions that found alleged disclosure of "highly personal or intimate" information such as healthcare information to be sufficient to state a claim for violation of the Right to Privacy Law, G.L. c. 214, § 1B, leaving as "question[s] of fact" whether the alleged intrusion upon the plaintiff's privacy through that disclosure was "unreasonable, substantial, or serious."
6. **Chapter 93A Claim:** The court was persuaded that disclosure of the plaintiff's private information contracted express promises, and so was an "unfair or deceptive act" subject to chapter 93A, and that a presuit demand letter that identified the plaintiff under her pseudonym was sufficient to satisfy 93A's presuit notice requirement.

In addition, the court dismissed negligence per se and invasion of privacy claims because Massachusetts law does not recognize those as standalone claims. The court declined to consider the hospital's arguments why the Massachusetts Wiretap Act claim should be dismissed, because that issue is currently before the SJC, and so that issue needed to be deferred.

National Law Review, Volume XIV, Number 138

Source URL: <https://natlawreview.com/article/healthcare-provider-beware-massachusetts-federal-court-largely-permits-tracking>