Beazley Logo

Article

Cyber risk revealed: Pixels and Tracking Technology

Katherine Heaton • December 14, 2022

Our cyber and technology claims specialists are seeing a significant recent increase in claims relating to pixels and other tracking cookies used on websites, particularly in the healthcare sector.

While new cyber threats are constantly emerging, this latest liability isn't caused by threat actors or cybercriminals, but internally - typically by unsuspecting marketing departments running online advertising campaigns with Facebook, Google, and others.

What is the risk?

Pixels are a code that can be embedded into a website to track a user's presence on the website; what they search for, pages they're looking at and interacting with, and even text entered into the website. Pixels are so common that the majority of websites are now using them. With the data they can collect, pixels offer huge potential to improve targeted marketing campaigns and increase a company's insight into its customers.

The pixel that has been the focus of a lot of the recent litigation and regulatory inquiry is the Meta pixel which tracks and collects user data, and then shares it with Facebook and Instagram, enabling highly targeted digital advertising to appear in the user's profiles.

For companies in the US Healthcare sector, this is causing a big issue.

How pixels are being used:

Hospitals are using pixels to voluntarily send data from users of their websites to Meta, Google, and others to help them with targeted advertising. Some hospitals only have pixels embedded on their forward-facing public website, but some have pixels on their patient portals as well.

The issue is that by sending information about website users to Facebook and other third parties, hospitals may be sharing Protected Health Information (PHI) with third parties without patient consent. This issue is acute when pixels are on patient portals, but PHI can be collected when pixels are just on the forward-facing public websites. Even when such sharing is inadvertent, it can lead to significant liability under HIPAA, state laws, and common law torts.

Retailers and other companies that use websites to advertise themselves, or to conduct business, are also using pixels to send data to Meta, Google, and others to help them with targeted advertising. For example, some companies that sell products online use pixels to capture data about products a website user may have viewed so that the product can be advertised to that user in their Facebook or Instagram feed.

Potential liability and impact threat:

When companies are thinking about implementing these technologies, they are thinking about the benefits. But with the rise in liability, there is a potentially significant risk that should be considered carefully.

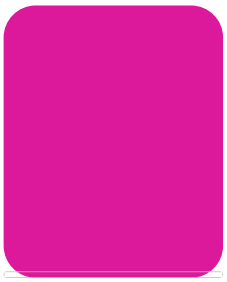
In June 2022, The Markup published an article warning that they had determined that 33 of the top 100 hospitals were using pixels on their websites. Since that article was published, more than 30 class actions have been filed against hospitals alleging various state statutory, contract, and tort claims based on the alleged sharing of PHI without patient consent. Thus far, most of these class actions are surviving motions to dismiss and courts seem to be taking a stern view of the potential sharing of PHI for targeted advertising. To date, only one hospital has settled its class action and that settlement was for around $18 million. We anticipate that the number of class actions will continue to grow and that the cost to defend and settle will be significant. There is also the potential for regulatory scrutiny as regulators are increasingly interested in privacy policies and how entities treat data, particularly when it comes to novel technology.

Additionally, there has been a recent increase in claims being filed against retailers and other companies that use pixels for targeted advertising or to assist with their website's "chatbot" feature. These claims are being brought under state wiretapping statutes, alleging that the pixels are intercepting communications and sharing with a third party without consent.

In August 2022, the Third Circuit Court of Appeals issued a decision holding that the use of pixels to send an individual's product search history to Facebook for targeted advertising could be considered an "interception" of a "communication" in violation of Pennsylvania's wiretapping statute. Since that decision was issued, there has been a surge of class actions alleging wiretapping violations being filed in Pennsylvania, California, Washington, and other jurisdictions. The wiretapping class actions are costly to settle because wiretapping statutes carry per-violation penalties of $1,000 or more, depending on the statute and level of culpability.

How to mitigate the risks:

- Take an enterprise view of risk and compliance when it comes to how you grow your business and engage with customers in the digital space.
- Ensure that legal and risk teams are working with marketing to see what technology they are using and how they are collecting, using and retaining data for targeted advertising.
- Liaise with third party marketing agencies to understand data collection and contracts.



Katherine Heaton

Claims Focus Group Leader - Cyber Services & InfoSec Claims

https://themarkup.org/blacklight

If a company determines that they want to use pixels despite the risk, they should engage an outside privacy expert to help them determine how to place the pixels on their websites and to craft notice/consents that can help minimize liability. Review carefully the OCR guidance on tracking pixels: https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html

Note that after you have a better understanding of your pixel risk, you should work with your broker to understand if there are coverage limitations depending on the type of risk, type of action and type of policy at issu

The information set forth in this document is intended as general risk management information. It is made available with the understanding that Beazley does not render legal services or advice. It should not be considered or relied upon as legal advice in any specific situation and Beazley does not guarantee the accuracy or completeness of any information or that the application of such information will avoid any loss. Each reader is responsible for determining the adequacy and appropriateness of any information he or she chooses to rely upon. Beazley accepts no responsibility for any errors it may contain or for any losses allegedly attributable to this information.

Home

©Beazley Group | LLOYD's Underwriters