Courtesy of
SCS Agency Inc

The Risks and Legal Implications of Pixels and Tracking Technology

A pixel refers to a small, transparent snippet of embedded code that enables digital tracking capabilities when a user engages in certain online activities, such as opening an email or visiting a website. Companies and their marketing departments have increasingly employed such code to analyze users' online behaviors, conversions and preferences (e.g., page interactions, search history and text entered within forms); gain detailed insights on potential customers; and launch targeted advertising campaigns across search engines and social media platforms.

Although pixels can prove useful for businesses, they also carry a wide range of risks, especially pertaining to data collection and processing. In particular, companies that utilize pixels could be more susceptible to data privacy concerns, regulatory exposures and cybersecurity threats. With this in mind, it's crucial for businesses to better understand these issues and take steps to mitigate them. This article provides more information on the risks and legal implications of pixels and tracking technology and outlines tactics companies can implement to reduce related exposures.

Data Privacy Concerns

Pixels usually present themselves as minuscule and undetectable image files within the content body of emails or websites, often harvesting data regarding users' digital activities without their knowledge or consent. What's more, businesses that leverage pixels may share the data they gather with third parties (e.g., Google and Meta) to assist them in creating targeted online advertisements. This means that the implementation of pixels can result in users unknowingly providing sensitive information to multiple parties, posing serious data privacy concerns. Pixel utilization and its related concerns are widespread; in fact, recent research from online messaging service HEY found that nearly two-thirds of the emails sent to users' private inboxes contain pixels.

Data privacy concerns may arise for any business that utilizes pixels but can be particularly prevalent among health care organizations. After all, when visiting these organizations' websites, users are more likely to disclose protected health information (PHI) and personally identifiable information (PII), including their names, contact details, Social Security numbers and medical records. According to nonprofit publication The Markup, one-third of the top 100 hospitals currently employ pixels within their websites; some of these organizations have even provided the data users stored in password-protected patient portals to large-scale social media platforms without their consent, which is both controversial and illegal.

Regulatory Exposures

Pixels also come with a variety of legal implications and regulatory exposures. Specifically, businesses that leverage this tracking technology may need to comply with the following legislation:

- **The General Data Protection Regulation (GDPR)**—For businesses that engage in international operations, Europe's GDPR prohibits the utilization of pixels across websites and other online platforms unless users consent to their data being collected by such technology.
- **The California Privacy Rights Act (CPRA)**—For businesses that service California residents, the CPRA requires users to be notified of the implementation of pixels and how the data this technology collects will be processed, including whether it will be shared with third parties. Upon

receiving this notification, users have the right to opt out of having their information disclosed via pixels.

- **The Health Insurance Portability and Accountability Act (HIPAA)**—HIPAA is a federal law that establishes standards for health care organizations to follow regarding the protection of individuals' PHI. According to guidance issued by both the Department of Health and Human Services' Office for Civil Rights and the Federal Trade Commission, utilizing pixels in a way that exposes users' PHI to third parties is a HIPAA violation.

Businesses have also been encountering litigation related to the use of pixels. In 2022, the 3rd U.S. Circuit Court of Appeals ruled that the utilization of pixels to disclose users' online search history with third parties for targeted advertising purposes violates Pennsylvania's wiretapping statute. Since this decision, more than 50 class action lawsuits involving similar concerns have been filed across multiple states, with some of these cases resulting in multimillion-dollar settlements.

Cybersecurity Threats

Apart from data privacy concerns and regulatory exposures, businesses that leverage pixels could face increased cybersecurity threats. Namely, cybercriminals may be more likely to target companies that utilize pixels in data breaches. For instance, cybercriminals could exploit vulnerabilities in a company's website to inject malicious pixels. These pixels could be designed to gather sensitive information, install malware or redirect users to phishing scams, causing a data breach.

Additionally, pixels don't always operate correctly, particularly when used in conjunction with third-party services that process large amounts of data daily. Misconfigured pixels can lead to information being disclosed to unauthorized servers, therefore compromising companies' overall security capabilities. For example, a recent malfunction in Meta's tracking technology, known as the Meta Pixel, resulted in multiple data breaches across several businesses and websites, exposing the sensitive information (including PHI and PII) of more than 5 million users. In any case, data breaches stemming from the use of pixels can leave businesses with major reputational and financial losses.

Steps Businesses Can Take

In light of the risks associated with pixels, here are some steps businesses can take to mitigate their exposures:

- **Weigh the pros and cons.** First and foremost, businesses should consult their senior leadership teams, marketing departments, IT experts and legal counsel to assess the pros and cons of implementing pixels within their digital operations. Based on companies' available resources and risk management capabilities, the exposures related to pixels may outweigh the benefits. In these instances, businesses should consider alternative digital marketing strategies and solutions that don't rely on pixels (e.g., contextual advertising) and limit the utilization of third-party tracking technology on websites.
- **Maintain compliance.** If businesses decide to utilize pixels, they should carefully review applicable data privacy laws and ensure compliance with this legislation. Depending on their jurisdictions' particular legal requirements, companies' compliance considerations may include publishing easily accessible data privacy policies on their websites; deploying consent pop-ups or opt-out messages that give users a chance to either accept or reject the use of tracking technology to collect and process their information; and establishing clear contracts with third parties that outline proper data protection and liability guidelines.
- **Secure proper coverage.** Lastly, businesses should purchase ample cyber insurance to maintain financial protection against losses that may result from pixel use. Companies can consult trusted insurance professionals to discuss their specific coverage needs.

Conclusion

Pixels can pose several different risks for businesses. By understanding these exposures and implementing measures to minimize them, companies can effectively leverage this tracking technology.

Contact us today for more risk management guidance.