Courtesy of
Venbrook Insurance Services

CYBERRISKS&LIABILITIES_

Wrongful Collection of Data Explained

Businesses of all sizes and sectors may be subject to unlawful data processing claims. According to the International Association of Privacy Professionals, lawsuits focusing on whether businesses lawfully collect and use personal data have been steadily increasing. These claims can cause significant financial and reputational damage to companies.

As businesses analyze the risks associated with personal data collection, they must be familiar with an evolving regulatory landscape and take steps to address their exposures. This article provides more information on what wrongful data collection is and areas of concern. It also provides tips for businesses to mitigate the risks associated with wrongful data collection.

What Is Wrongful Data Collection?
What constitutes wrongful, or unlawful, data collection varies by jurisdiction. While there currently isn't an overarching national consumer data privacy law in the United States, several states have enacted legislation that affords individuals those protections. Aspects of U.S. laws also apply to certain sectors (e.g., the Health Insurance Portability and Accountability Act, or HIPAA, applies to health care) and individuals (e.g., children receive data protection through the Children's Online Privacy Protection Act). Additionally, different laws are in place internationally. This range of legislation can make it difficult for businesses to understand the various rules that are in effect.

Even though it may be complicated, businesses have the duty to comply with applicable data privacy laws. For example, depending on the jurisdiction, there may be regulations that dictate how or if an organization may collect, use and share personal data. There may also be requirements for the business to inform consumers that data is being collected and to allow the consumer to opt out of that collection. Failure to adhere to relevant laws may be considered wrongful and businesses may be subject to fines and potential litigation.

Areas of Concern
Certain aspects of personal data collection are areas of concern. Examples of areas laws may regulate include:

- **Biometric data**—Collection of data regarding unique physical characteristics (e.g., fingerprints, faces, voice patterns) has been regulated by some jurisdictions. For example, Illinois has enacted the Biometric Privacy Act, which forbids businesses from collecting biometric data unless the business has informed the individual about the data being collected, provided information on how long it will be stored and received written consent.
- **Pixel tracking**—The use of pixel technology to track how individuals use websites to target advertisements may be subject to regulations. For example, under the European Union's General Data Protection Regulation, pixel tracking technology may only be used if an individual consents, while the California Privacy Rights Act (CPRA) requires users to be notified of the implementation of pixels and how they will be processed.

  Additionally, the United States Video Privacy Protection Act (1988), originally enacted to prevent the disclosure of personal information obtained from renting videos, has seen a modern application in lawsuits involving data collected through pixel tracking. Furthermore, HIPAA can be used to safeguard patients' confidential health data that may be exposed to third parties utilizing pixels.
- **Genetic information**—Data that is compiled from the analysis of a person's biological sample and involves genetic material (e.g., DNA, genes, chromosomes)

VENBROOK
INSURANCE SERVICES

may also be subject to regulations. For example, the Genetic Information Privacy Act in California provides its residents with rights and protections over their data when they use direct-to-consumer genetic testing companies.

- **Precise geolocation**—There may be legal obligations regarding collecting and processing data that is used to locate a consumer within a specific area. For example, the CPRA requires individuals to receive notice and the right to limit the use and disclosure of that precise geolocation information.

Risk Mitigation Strategies

It is essential for businesses to implement risk management strategies to reduce the likelihood of lawsuits, reputational damage, and regulatory fines and penalties stemming from wrongful data collection claims. Examples of techniques to consider include:

- **Weigh the benefits and drawbacks** of data collection and determine if alternative marketing strategies that do not require data collection exist.
- **Provide notice and obtain consent** before collecting, processing, using, sharing or selling personal data.
- **Allow individuals to opt out** of having their personal data collected.
- **Limit personal data collection** to only what is necessary.
- **Monitor regulations** as they are quickly evolving.
- **Conduct audits** of data collection practices to ensure they conform to applicable regulations.
- **Provide education** to employees on proper technology use and applicable legislation.
- **Review insurance coverage** with a licensed professional to determine if coverage is available for wrongful data collection claims.

Conclusion

Claims of wrongful data collection are rising, and businesses should take steps to mitigate their exposure to this risk. For more information and risk management guidance, contact us today.