U.S. Risk, LLC

PRIVACY UPDATE: WRONGFUL DATA COLLECTION

Who we call, where we drive, what messages we send – all are collected, used and potentially shared. With increased focus on wrongful data collection and privacy concerns, compliance is essential in mitigating risk.

KEY AREAS OF CONCERN

Wrongful collection of protected health information (PHI) and personally identifiable information (PII) without proper consents or releases are creating dramatic increases in regulatory claims. How information is collected and used is of increasing importance to the FTC and other governmental bodies. GDPR (European General Data Protection Regulations), CCPA (California Consumer Privacy Act) and other state laws have created awareness of the problems surrounding wrongful collection of PII and PHI. While there is no comprehensive federal law yet regulating the collection, processing, disclosure and security of personal information, there are efforts underway by the FTC to look at commercial surveillance and data security practices. In addition, there is a fast-growing maze of federal and state laws, particularly those focused on newer technologies such as biometrics.

› Biometrics Data

The use of biometric data is a complex issue involving security, privacy, and consent that has been, until recently, largely unregulated. Biometric privacy laws generally require businesses to track, inform employees or consumers of, and provide methods for employees or consumers to consent to the collection of biometric information or biometric identifiers. They typically must provide notice, obtain written consent and make certain disclosures before they can collect, use or store this data. Biometric laws can impact both cyber and employment practices liability (EPL) coverage, so businesses need to be aware of their obligations as non-compliance can create significant exposure.

› Geolocation Data

How geolocation data is tracked and used is also a key concern. Geolocation makes it possible from any device connected to the internet to obtain all types of information in real time, locating the user with pinpoint accuracy, determining patterns and behaviors. More than 90% of the apps installed on smartphones use geolocation. A recent privacy case explicitly mentioned geolocation as used to track an individual to a health care clinic. Many states have introduced or in the process of crafting comprehensive consumer data privacy laws, with proposed federal legislation seeking to regulate and apply greater scrutiny to privacy practices. The tipping point for a dramatic rise in lawsuits could be the massive Google settlement lrelating to geolocation—the largest privacy-related settlement to date.

› Opt In/Opt Out Disclosures

A large part of wrongful data collection focuses on nondisclosure of opt in/opt out privacy. Opt-in means that users have their consent to collect and use personal data. Opt-out means that users have withdrawn or refused content. In both cases, these are actions that individual has specifically taken to consent or refuse. Companies must be transparent in how they track customers, give users detailed information and gain permissions, abiding by state and federal privacy laws.

U.S. Risk, LLC

PRIVACY UPDATE: WRONGFUL DATA COLLECTION

CHECKLIST

Many insurers are requesting more details information about data collection, use and sharing.
Some of the most common questions include:

- ☑ Do you collect any data or information that isn't reasonably required to complete a transaction or provide a service?
- ☑ Do you publish or distribute any computer or cell phone apps?
- ☑ Do you collect geolocation information?
- ☑ Do you collect or use any biometric data?
- ☑ Do you collect information pertaining for children or minors?
- ☑ Do you obtain explicit consent or release from each individual for the collection and use of information, including biometric data?
- ☑ Do you publish a privacy policy?
- ☑ Do you sell any type of data? Do you buy any type of data?
- ☑ Do you enable users to log in or authenticate to any online services using account credentials associated with social media?
- ☑ Do you use software or analytical tools that track the activities of website visitors or other third-party users of its computer systems?
- ☑ Do you use tracking pixels on any website or marketing emails that capture user data and shares it with a third party?

Responses to these questions could lead to a wrongful collection exclusion. Sample wording reads like this:

It is hereby understood and agreed that the coverage under this Policy shall not apply to any claims, losses, damages, claim expenses, or other amounts, arising out of or resulting, directly or indirectly, regardless of any other cause occurring in any sequence, from the unlawful or allegedly unlawful collection, use, processing, retention, storage or disposal of Private Information, including, but not limited to, any actual or alleged failure to provide required notice of, or obtain required consent for, such practices.

In addition, the defined section of the policy is amended to include the definition of private information:

1. Confidential information of a third party; or,
2. Information that can be used to determine an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual or household; that is in the care, custody or control of the Insured, or a third party on behalf of the Insured.

THE BOTTOM LINE

A thorough review of policies with respect to wrongful collection is more important than ever. Exposures will only increase and even the most diligent organization can be susceptible to a claim. A trusted expert highly experienced in cyber policy wording and how to customize policy terms should be brought into the process as early as possible to help clients assess their exposure in this fast-changing arena and ensure coverage for critical risks, future potential claims management, and the latest developments in terms and conditions.