Sedgwick LLP

10 Ways To Avoid Wrongful Collection Of Data Claims

Today's technology allows businesses an intimate look into the lives of their customers. Answering the questions of the who, what, where, when and why of consumers, has become increasingly easier. Knowing the answers to these essential questions about consumers, allows businesses to engage in targeted marketing, which ultimately leads to more business. As the value of consumer data and data security threats increase, national governments (U.S. and abroad) and states have enacted and vigilantly enforced regulations relating to the collection and processing of consumer data.

Two recent matters shed light on the Federal Trade Commission's enforcement and protection against the wrongful collection of consumer data. In June 2016, the FTC filed a complaint against InMobi Pte Ltd. in the United States District Court for the Northern District of California for violations of Section 5(a) of the Federal Trade Commission Act (which prohibits unfair or deceptive practices or acts affecting commerce) and the Children's Online Privacy Protection Act alleging that it improperly collected data regarding users' GPS locations. InMobi settled with the FTC for a $4 million civil penalty, which was suspended to $950,000 because of the company's financial condition.

In December 2016, the FTC filed an administrative complaint against Turn Inc. for violation of Section 5 of the FTC Act because it allegedly improperly collected customer information by misrepresenting how customers could restrict the ability to be tracked. Although the FTC did not impose a monetary fine, the proposed consent order bars Turn Inc. from improperly tracking customers and requires compliance with the consent order's compliance terms for a 10-year period. These FTC actions shed light on the risk of wrongful collection of data claims companies may face.

Here are 10 tips to avoid the ever-increasing wrongful collection of data claims:

1. Understand What's Collected, Processed and Stored

It is important that companies have a strong grasp on the data they collect, process and store and the regulations that their practices are subject to. Sensitive data mapping is an essential first step in avoiding wrongful collection claims because it allows a company to ensure that its notices and consents are in line with current practices and applicable regulations.

2. Do Not Hide the Details

A company's privacy notice should be easy to find and understand. The privacy notice should explain what information is collected, how it is collected, how the information is used, and inform customers how to access the information held by the company. A good defense against a wrongful collection claim starts with a privacy notice that educates the consumer on how the company collects and processes data.

3. Opt-In Versus Opt-Out

Federal and state regulations impose different obligations regarding whether an opt-in is required or if an opt-out is sufficient. It is important to understand and know the difference. For example, an opt-in is typically required for a substantive retroactive change to a privacy policy, but an opt-out may be sufficient if the change is not material.

Originally published on *Law360*, February 7, 2017. Posted with permission.(subscription required)

4. Understand Who the Company Answers To

The expanding regulatory landscape is also creating stronger regulatory enforcement. It is important for a company to understand which regulators it answers to and how regulations vary. For example, a company may or may not fall under a state privacy and data-collection regulation or the regulation in one state may be stricter than in another. Companies must map out their various compliance obligations to ensure they comply across the board, domestically and abroad.

5. Do Not Forget About Your Vendors

An example is the 2013 Target breach. The most surprising fact of that breach, is not that it happened, but that the hackers used one of Target's heating, ventilation and air conditioning (HVAC) vendors to infiltrate the system. Although a company may have a handle on its own practices, companies should review the practices of its vendors. Notably, this is also an area of increased enforcement by regulators.

6. Keep an Open Line of Communication with Consumers

It is important that companies provide consumers with a clear and open line of communication to address concerns about data collection and privacy. This is the first step to helping prevent consumer complaints and ultimately protect the company brand.

7. It Takes a Team

Data collection is not just a business decision and data security is not just an information technology issue. Companies must ensure that their internal teams work together and take ownership over their respective roles in the collection, processing and protection of consumer data. For instance, the research and development team may come up with a great new feature to the company's mobile application that stores a customer's location for convenience, but it takes members from the information technology, systems and security teams to ensure that data is protected and from the business unit to ensure the application operates in a way that is consistent with the company's data practices and policies. It is important that these teams work collaboratively to ensure the collection and protection of consumer data.

8. Look Internally

Collection is not just about receiving information from a consumer, but also looking at how that information is shared between departments within a company. Data may only be used for the purpose for which it was collected. Therefore, a company may be subject to a wrongful collection claim if department X collects data for a certain purpose and shares the data with department Y, which uses the data for a different purpose. Privacy notices and consents should reflect the purposes for which the data may be used across the company.

9. Choose a Diet the Company Can Stick To

Many data security experts will tell you that the best way to avoid claims related to data collection or security is to not have the data in the first instance. A "data diet" requires the company to look at the data points that are necessary to service customers and revise its data-collection practices to reflect the actual needs of the business.

10. Review, Revise, Execute

Technology changes at an incredibly rapid pace. It is important that companies continuously review their data-collection practices, policies, notices and consents to ensure they reflect their current practice and regulatory compliance. Equally important

is for companies to remain vigilant of the changes in the law and emerging risks, which may trigger further updates to data-collection practices, and perhaps also changes to their business practices.

About the Authors

Cinthia Granados Motley
Partner
Chicago
312.641.9050
cinthia.motley@sedgwicklaw.com

Ashley S.A. Jackson
Associate
Chicago
312.641.9050
ashley.jackson@sedgwicklaw.com