BRANN & ISAACSON
ATTORNEYS AND COUNSELORS AT LAW

January 7, 2019

BRANN & ISAACSON CLIENT ALERT: PRIVACY IN THE CROSSHAIRS

The Issue

In the modern online marketplace, vast amounts of information, both personalized and anonymous, are collected, analyzed, transferred, and shared using a variety of technologies. Keeping abreast of the latest privacy and data security law developments is more critical than ever.

What You Need To Know

Given the national, even international, scope of your customer base, it is necessary to keep an eye not just on privacy developments in federal law, but state and international requirements as well. The risk is not just from regulators. Increasingly, class action lawyers are attacking direct marketers and their service providers for alleged privacy and information security violations, including in states where the potential recovery can be thousands of dollars for each violation, and total amounts sought can be staggering.

California became the first state to create privacy obligations for all websites when it enacted the Online Privacy Protection Act (Ca. Bus. & Prof. Code §2257 *et seq*.), requiring operators of commercial websites who collect personal information about California customers to post a privacy policy, accessible from the website's homepage. Although privacy policies were fairly common at the time, in part to fend off threats of federal legislation, the California law amounted to a *de facto* nationwide requirement, and privacy policies are now a standard component of essentially all commercial websites.

In recent years, there have been several developments with potential repercussions for the privacy policies of U.S. retailers, including:

1. Advances in advertising technology, including the widespread use of third–party services such as Google Analytics for targeted advertising;
2. The **European Union's General Data Protection Regulation** ("GDPR"); and
3. California's recent passage of the **California Consumer Privacy Act of 2018** (the "CCPA"), which will take effect on January 1, 2020, but which may be further amended before it becomes effective. Indeed, certain clarifying amendments to the original Act have already passed.

Action Items

First, as analytics tools become more sophisticated, new and more detailed disclosures in the privacy policy may be appropriate—including as to the means and manner of information collection, the uses of such information, and consumer options to limit such uses. In some cases, the maintenance of a privacy policy with specific disclosures may be a condition of utilizing the services. The terms of service for Google Analytics, for example, provides in relevant part that a user "must disclose the use of Google Analytics, and how it collects and processes data." Facebook's "Business Tools Terms" requires a similar disclosure, noting that "[i]f you use our pixels or SDKs, you further represent and warrant that you have provided robust and sufficiently prominent notice to users regarding the Customer Data collection, sharing and usage," spelling out particular requirements for websites and apps.

At the same time, the question of whether and how to obtain the agreement of website visitors to such practices is becoming increasingly important. The mere presence of a privacy policy link at the bottom of a web page may provide less protection than many retailers realize. The GDPR, for example, prohibits collection of personal data without a lawful basis, such as the consent of the individual whose data is being collected. Since the GDPR took effect in May 2018, many website operators have implemented pop-up messages advising website visitors of their data collection and cookie practices, and seeking affirmative consent to these practices.

Second, the EU and California requirements have implications not only for the contents of a privacy policy, but for data practices more generally. The GDPR, for example, provides EU residents with certain affirmative rights regarding their data, including:

1. Right of access to personal data;
2. Right to "rectify" or correct inaccurate personal data;
3. Right to demand erasure of personal data ("Right to be forgotten"); and
4. Right of data portability.

You should know that there is an argument that the GDPR does not apply to U.S. companies that are not actively targeting customers in the EU, nor using data collected from website visitors to target advertising specifically to EU customers. However, if it should apply, the GDPR imposes very strict notification timelines for data breaches affecting EU residents, and requires appointment of a representative in Europe. Moreover, regardless of whether a particular U.S. company is subject to the requirements of the GDPR, all fifty U.S. states already have some form of data breach notification law on the books.

The CCPA provides similar rights to California residents, including, but not limited to:

1. Right to request from a business "the categories and specific pieces of personal information the business has collected;"
2. Right to request that a business delete any personal information about the consumer which the business has collected from the consumer;
3. The right to opt–out of the sale of their personal information; and
4. A private right of action for consumers whose data was exposed in a data breach, with the potential to recover actual damages or statutory damages of between $100 and $750 per incident.

California's new regulation applies to companies doing business in the State that collect consumers' personal information and that satisfy one of the following: (a) have $25M annual gross revenues; or (b) annually buy, receive, sell or share for commercial purposes the personal information of 50,000 or more consumers, households, or devices; or (c) derive 50 percent or more of their annual revenues from selling consumers' personal information.

Full compliance with the CCPA will stretch beyond updated privacy policies and informational disclosures, and may include significant investments in IT and data security architecture as well as the training and implementation of staff to receive and handle consumer requests. Addressing these items is a larger issue that will require input from IT and other business stakeholders.

BRANN & ISAACSON advises online retailers on a range of data privacy and security issues, including changing legal requirements around data practices and disclosures and data breach response. This alert is intended as a high–level summary of issues on the horizon that could affect your privacy practices and policies. It is not intended as an in–depth analysis of the legal requirements applicable to particular businesses or industries.

If you have specific questions about this client alert or data privacy or security issues particular to your business, don't hesitate to contact a member of our team: David Bertoni (dbertoni@brannlaw.com); David Swetnam–Burland (dsb@brannlaw.com); Stacy Stitham (sstitham@brannlaw.com); or Nat Bessey (nbessey@brannlaw.com); or reach out to us by phone at (207) 786–3566.