

CORPORATE COUNSEL

An **ALM** Website

corpcounsel.com | August 1, 2016

Tax Reporting Laws Raise Privacy Claim Risks for Online Companies

Marvin Kirsner and Elizabeth Rogers

States are scrambling to shore up sales tax revenues that are eroding because of e-commerce sales. A new approach to sales tax collections involves information reports on customers' online purchases. This approach may create potential legal claims against many online companies for giving too much information about customers to state tax agencies or even to the customers themselves. Companies potentially affected include any e-commerce business selling goods or taxable services, companies that sell digital products through electronic download or streaming service, cloud computing companies, and brick and mortar retailers that do not have stores in the state but deliver products there.

Because of U.S. Supreme Court precedent, brick and mortar companies and online companies are



required to collect sales tax on products and taxable services only when the customer is in a state where the company has a physical presence ("nexus"), either directly or through affiliates. Although companies without nexus in the state where a customer is located are not obligated to collect the sales tax, the customer is still obligated to pay the tax to the state herself.

In an effort to capture these unpaid sales taxes, there is an emerging trend: States are passing legislation that requires online companies to file information reports to help the states in getting its residents to pay the sales tax themselves. Colorado was the first state to pass this law in 2010. This law was challenged in the courts on the grounds that the state could

not require a retailer to comply with these information reporting rules if the retailer does not have nexus there. In February the U.S. Court of Appeals for the Tenth Circuit upheld the law, and in the four months since then, three additional states—Louisiana, Oklahoma and Vermont—have adopted variations of the Colorado law, signaling a legislative trend that additional states might follow.

There are two separate types of information reporting regimes. One only requires the company to send an annual notice to its customers to inform them how much their total purchases were during the year so that they will know how much tax to pay to the state. These are the so-called single report states—currently Oklahoma and Vermont. The second reporting regime requires a report to the state tax agency in addition to a report to the customer—so that the state tax agency will know how much tax the customer should be paying. These double report states are currently Colorado and Louisiana.

Prior to this trend, the collection of sales tax from customers had not involved the disclosure of the names of the companies' customers to state tax agencies. Customers purchase products online for a variety of reasons, but usually the transactions

purposely occur in a controlled and nonpublic setting that provides for a transaction that is anonymous with regard to any third party, most especially a state government agency. Furthermore, some customers make purchases online in order to keep sensitive purchases undisclosed to their significant others, family members and/or employers (think about a man who purchases sexy lingerie as a gift for someone who is not currently his significant other).

The expectation of privacy to which these customers have become accustomed, by making online purchases in a non-public setting, is about to be upset by the enforcement of these new regimes. For example, if a customer has not paid tax on a purchase in a double report state, the customer can expect an assessment notice from the tax agency for back taxes based on the notice that the online business is required to file. The notice serves as a collection tool for the state, but in the process also requires a breach of the traditional online retailer-customer anonymity, because the states will now know the name of the online retailer from which the customer made the purchases. Potentially, there will be intra-family and employment privacy concerns in the single report

states as well, because notices will be sent to the mailing address of the customer, which would typically be either a residence or place of employment.

The double report laws both say that the retailer is to report to the state tax agency only the total dollar sales to each customer in the state. Acknowledging privacy concerns, these two statutes prohibit a description of the specific items purchased. A possible risk faced by online retailers is that staff, who are not familiar with the prohibition against reporting detailed purchase information, might simply file a report from its records that identifies the products. These additional disclosures that are not required by law, in turn, could lead to litigation against the online retailer, claiming (i) a data breach based on disclosure of any element of personal identifiable information or personal health information (as defined by state breach notification statutes); (ii) breach of privacy (under common law theories of invasion of privacy); (iii) breach of the Health Insurance Portability and Accountability Act (HIPAA) and its state law counterparts, which prohibit the disclosure of an individual's personal health information, if information contained in the report indicates that the transaction relates to

the health condition of the customer (i.e., prescriptions, medical devices, etc.); and, (iv) violation of the Video Privacy Protection Act (protecting consumers' privacy with regard to videotapes they rent or purchase).

Furthermore, online companies that voluntarily add information beyond which the law requires may risk violating their own website privacy policy by sharing information that is inconsistent with what the policy states. The Federal Trade Commission considers practices that are inconsistent with written statement in a privacy policy to constitute deceptive and unfair behavior under Section 5 of the Federal Trade Commission Act; thus, such voluntary reporting of transaction details beyond that required by law could expose these online retailers to enforcement actions and fines and penalties by the FTC.

To complicate matters, the Colorado law requires the company to give a description of the items purchased in its report to its customers. As a result, by law, the report to the customer (including the detailed information) and the report to the state (which prohibits this detailed information) will have to contain different information, or risk a privacy breach claim.

The Oklahoma law (a single report state) expressly prohibits any identification of the products purchased in the required reports to customers—an apparent acknowledgement of potential invasion of common law or statutory rights of privacy in the context of intrafamily or employer-related confidentiality concerns. The risk of exposure for privacy-related litigation increases if a company innocently sends to its Oklahoma customers the same detailed listing that it must send to its customers in the double report states.

Because of the potential that class action claims will give more information than the law requires, GCs should be involved in setting up these information reporting compliance protocols. Companies that are required to file these tax information reports might find themselves between a rock and hard place when it comes to complying with these rules. If they give more information than the law requires, they will risk facing privacy breach claims. On the other hand, if they do not provide adequate information, they will face potential penalties from the state tax agencies. This conundrum is analogous to the class action claims in which many companies have become embroiled for collecting

more sales tax than required by law. The GC's direct involvement in this information reporting process could be critical in managing these potential risks.

It is possible that potential privacy concerns might ultimately force some retailers to voluntarily agree to collect the tax from their customers, even if they are not required to do so because they do not have nexus. And perhaps this is the silent goal of these new laws: The states are implicitly saying, "If you don't collect the tax, you are going to have to report information and aggravate your customers, so it might just be easier to collect the tax even though you are not required to do so." GCs should have a role in any such decision-making process.

***Marvin Kirsner** is shareholder in the tax department of Greenberg Traurig, focusing on e-commerce and technology-related tax issues. **Elizabeth Rogers** is a shareholder in the firm's IP and technology department. She focuses on cybersecurity, privacy and data security issues. She was the chief privacy officer for the Texas Comptroller of Public Accounts prior to joining Greenberg Traurig.*