DATA PRIVACY: Responding to Law-Enforcement Requests

by Reggie Pack

Over the last handful of years, data/information privacy has become a mainstream, hot-button topic. Most of the time, data privacy news surrounds the most recent data breach, targeted advertising scheme, or an unauthorized/undisclosed data sharing arrangement between giant corporations.

As a business owner, each of these situations are worth being concerned about, but they are not the only data privacy concerns you need to prepare for.

For example, during its most recent session, the Utah legislature passed several amendments to the Utah "Electronic Information or Privacy Act." Within this act, rules are enumerated for how and when governmental agencies—and law enforcement agencies in particular—can force a business to divulge certain electronic data records about its customers.

Generally, the act requires a "warrant based on probable cause" to demand such records. However, the act also includes numerous carve outs to the warrant requirement. In certain instances, the holder of the record (the business) may be able to "voluntarily" hand over the records. However, doing this may result in you running afoul of your current customer privacy policy.

As can be appreciated, this privacy wrinkle is notably different from the typical breach-type privacy issues your company has likely considered. Also, because the US lacks a wide-reaching federal information privacy policy, different states have different requirements for such requests. As a business owner and holder of customer records, you should be aware of individual state requirements where you operate, how to comply with those requirements, and how to protect your customer information (and, by implication, your customers) in view of those requirements.

If you are unprepared, receiving a governmental data request may quickly become a lose-lose situation. If you turn the data over too easily, your customers may be angry. However, if you fail to comply with a properly supported demand, you may face penalties, fines, or other

consequences.

To this end, the following items are things you should consider and/or implement to ensure your business is in the best position to respond when a governmental entity comes knocking:

1. Establish a clear and concise protocol for reviewing governmental data access requests. Your protocol should identify company officials that can rapidly make high level decisions.
2. Understand the full range of data that you collect and maintain about your customers. Limit the type of data you maintain to limit your overall exposure to such requests. Establish technical means to ensure you don't share unrequested data, to the extent possible.
3. Determine, before a request comes, your "voluntary disclosure" policy.
4. Ensure your customer-facing privacy policies are clear. For example, in addition to including the ways you technically protect user data (e.g., encryption, physical access controls, etc.) also disclose your protocol for responding to data access requests, including your policy for voluntary disclosure for governmental requests (item 3 above).
5. Maintain robust records associated with any data request including when the request was made, whether it was accompanied by a warrant, whether/how you followed your pre-established protocols for handling requests, and whether/how you met your obligations to your customer with respect to the request.
6. Have your technology privacy counsel on speed-dial in case you run into questions.

Data privacy is a complicated and rapidly changing consideration for your business. Understanding all of the ways your customer data is at risk is essential for keeping your customers happy and your business successful. If you have questions about data privacy, Workman Nydegger is here to help. We have extensive experience in helping customers establish data privacy protocols and compliance documentation to ensure that you are prepared to effectively respond when a data privacy event occurs.