Why So BLU?: FTC Settles Privacy and Data Security Claims with Mobile Company; Fencing-In Relief Requires Consumer Opt-In to Data Sharing

Alysa Z. Hutnik, Dana B. Rosenfeld

May 2, 2018

Earlier this week, the FTC settled its case with BLU Products, Inc., a cell phone company the FTC claimed misled consumers about its privacy and data security practices. According to the agency, the company represented that it did not collect unnecessary personal information and that it imposed specific data security procedures to protect consumers' personal information. But the FTC claimed not so fast, alleging that BLU allowed one of its partners, an advertising software company, to collect sensitive consumer information such as text message contents and call logs with full telephone numbers. The FTC also alleged that BLU failed to implement the security features it represented to consumers, allowing the company's devices to be subject to security vulnerabilities that could allow third parties to gain full access to the devices.

In settling the case, BLU agreed not to misrepresent its data collection or data security practices. The order also requires BLU to clearly and conspicuously disclose: (1) all of the "covered information" that the company collects, uses, or shares; (2) any third parties that will receive this "covered information"; and (3) all purposes for collecting, using, or sharing such information. This disclosure must be separate from the company's privacy policy or terms of use and the company must obtain the consumer's affirmative express consent to the collection, use, and sharing of such information. "Covered Information" is defined as geolocation information, text message content, audio conversations, photographs, or video communications from or about a consumer or their device.

The company is also required to implement a comprehensive security program, designed to address mobile device security risks and to protect the security, confidentiality, and integrity of consumers' information. Specifically, the order requires the company to:

- Designate an employee to be responsible for the program;
- Identify the internal and external risks to the security of the company's devices that could result in unauthorized access to them and assess the sufficiency of any safeguards;
- Design and implement reasonable safeguards to control the identified risks the company has identified;

- Regularly monitor the effectiveness of the safeguards' key controls, systems, and procedures;
- Develop and use reasonable steps to select and retain capable data security service providers that are required to implement appropriate safeguards; and
- Evaluate and adjust the security program based on any changes that could affect its effectiveness.

The order also provides specific requirements for biennial third-party assessments of the security program.

In a time when privacy and transparency remains a newsworthy topic, the FTC's most recent privacy settlement highlights the importance of accurately representing data collection and data security practices, and carefully considering whether an opt-in vs. opt-out is the reasonable choice, given the sensitivity of the data at issue. It's also a good reminder to understand what user or device-level data is being collected, including by vendors and marketing partners, and monitor such activity for compliance and risk management. As many companies have discovered, broader, unexpected consumer data collection and sharing can raise not only legal exposure, but significant negative PR for the brand.