New York AG Settles with School Calendar App, Saturn

Alysa Z. Hutnik, Paul L. Singer, Beth Bolen Chun, Abigail Stempson

March 12, 2025

This week, New York Attorney General Letitia James announced a settlement with app developer Saturn Technologies (Saturn) following an investigation into privacy practices that promised teens an exclusive community but allegedly did not deliver on its claims. The Assurance of Discontinuance (AOD) states that Saturn's actions constituted violations of New York's Executive Law 63(12) and General Business Law 349, its main UDAP statutes. Saturn must pay New York $200,000 (with an additional $450,000 payment suspended).

New York's Investigation and Allegations

Saturn's calendar app included social media components such as the ability to share personal info like name, picture, and school schedule, along with several messaging components. The app promised users, including in the privacy policy and FAQ, the info they shared was limited to students at their school, by verifying a user's email address. However, the AG investigation found that email verification practices were only required until summer 2021, and by August 2023, less than 30% of accounts on the app were verified by email.

While the app used substitute verification methods (in part to avoid a tech issue), the AG alleged they were not proven effective. Further, at times verification was not required at all, and the app specifically allowed "unverified" users. Unverified users could still see many of the same features as verified users, including certain chats, class schedules, and student bios of verified users. In addition, the app did not screen based on birth date (to block adult users) or location (to block users out of state) despite collecting location data for other purposes.

In August 2023, a social media watchdog group reviewed the app and expressed concerns, and a parent's social media post went viral expressing similar concerns. After widespread press coverage, Saturn announced changes to the app – including improved verification processes and segregating unverified users. But the AG alleged that some of the new verification methods, like a "friendship user verification," were not tested for effectiveness prior to implementation. When requesting access to phone contacts, even after Saturn made changes to its privacy policy, it did not disclose that the contacts would be copied and retained for future use, even if the user revoked device permissions.

Further, the AG also alleged that at least prior to August 2023, "Ambassador Program" promotions of the app by popular high school students did not disclose material connections (such as compensation through a rewards point system). Saturn did not provide the students with training or guidance on complying with advertising law.

Settlement Terms

The AOD broadly requires Saturn to comply with its UDAP laws and requires compliance with the

FTC's Endorsement Guides.

It further requires:

- Marketing training for employees and non-employees/Ambassadors on compliance with marketing laws and FTC Endorsement Guides
- Documentation of changes to policies, procedures, and codes related to data privacy
- Deletion of copies of contact books when users delete their account, and an account setting to revoke permission to access contacts and delete them
- Additional disclosures to and consent from existing users, including:
    - A clear disclosure that Saturn does not confirm users are students
    - Obtaining express consent from users to continue using the Saturn App given the above disclosures
    - Providing a link to an account deletion setting
    - Allowing users to review and edit their friends list
    - Clearly disclosing the option to adjust the current privacy settings
- The AG office must approve the user interface.
- New users under 18 to use a personal information settings process that includes clear and conspicuous descriptions of settings, confirmation of privacy options, and the clear and conspicuous disclosure that users may not be students. The default privacy settings for these users must hide social media links from non-friends.

The AOD prohibits:

- App users from accessing certain information about non-users – for example, non-app students' schedules
- Retaining phone contacts where a user previously revoked device permissions
- Unsubstantiated user safety claims
- Unsubstantiated user validation claims

Takeaways:

1. Ensure marketing claims keep up with changes to privacy features and settings.
2. States don't have to use comprehensive privacy statutes to tackle deceptive marketing claims about safety and privacy.
3. Don't let COPPA compliance make you lose sight of big picture UDAP compliance and privacy best practices.
4. Teen privacy remains a hot issue for AGs. AGs remain focused on social media's impact on teens. If you offer a product or service that potentially puts teens at risk of unwanted contact or potentially exposes their personal information, you should expect enforcers to take notice and

use their full authority to address their concerns.