

Breakfast with a NY A.G. Deputy Bureau Chief: Update on Data Breaches, COPPA and False Online Reviews

June 20, 2018 – The TMCA

by Adam Sapper



On June 13th, we hosted a “Meet the Regulators Breakfast” with Clark Russell, Deputy Bureau Chief of the Bureau of Internet and Technology of the NY State Office of the Attorney General, along with Dorsey’s privacy lawyer Bob Cattanch, which was sponsored by the Association of National Advertisers. For those of you who missed out on this event, never fear—the TMCA has you covered with a recap of a few of the highlights.

Related Capabilities

- Trademark, Copyright + Advertising
- Intellectual Property Litigation

Operation Child Tracker: The Children's Online Privacy Protection Act (COPPA) first went into effect in 2000 and is designed to protect the online privacy of children under 13. COPPA doesn't just cover operators whose websites or online services directly collect personal information from children—it also covers those whose sites and services integrate third party services (such as plug-ins or advertising networks) that collect personal information from underage visitors. And COPPA imposes *strict liability* on violators, so even if operators aren't aware that third party advertisers have installed tracking technologies that violate COPPA, the operators themselves are still liable. Deputy Bureau Chief Russell talked about Operation Child Tracker, a two-year, first-of-its-kind investigation by the AG's office, which ended in a number of settlements totaling \$835,000 with some of the nation's most popular kids' toy and media companies whose websites were home to third-party technologies that enabled the tracking of children's online activity in violation of COPPA.

Data Breaches: We couldn't have breakfast with the Deputy Bureau Chief of the Bureau of Internet and Technology without discussing data breaches! Deputy Bureau Chief Russell led us through the AG's 2017 report documenting the *record number* of data breach notices filed with the NY A.G.'s office in 2017. There were a total of 1,583

data breaches reported, exposing the personal records of 9.2 million New Yorkers, which is four times the number of those reported impacted in 2016. The report shows that in 2017, employee negligence (which encompasses inadvertent exposure of records, insider wrongdoing, and the loss of a device or media) accounted for 25% of reported breaches.

Operation Clean Turf: Deputy Bureau Chief Russell also discussed Operation Clean Turf and the AG's recent investigation into fake social media accounts. Operation Clean Turf was a year-long undercover investigation into the reputation management industry, astroturfing (*i.e.*, masking the true sponsor of a message to make it appear as though it originates from and is supported by a grassroots participant) and false endorsements. Operation Clean Turf specifically targeted the widespread practice of companies being paid to generate fake consumer reviews on websites such as Yelp and Google Local. During the course of the investigation, representatives from the AG's office, posing as an independent frozen yogurt shop in Brooklyn, called various search engine optimization (SEO) companies to request help with negative reviews of the yogurt shop on consumer-review websites. Many of the SEO companies offered to write fake positive reviews and post them on consumer-review websites as part of their standard reputation management services. These companies use advanced techniques to hide their identities and bypass consumer-review websites' filtering and fake review detection, even going so far as to pay freelancers in the Philippines, Bangladesh and Eastern Europe \$1 to \$10 per fake review posted. Operation Clean Turf resulted in 19 companies paying more than \$350,000 in penalties and agreeing to cease their practice of writing fake online reviews for businesses.

But fake reviews aren't the only issue: companies are also using techniques to encourage would-be positive reviewers to post reviews, while filtering would-be negative reviewers away from review sites. Deputy Bureau Chief Russell pointed to one example in which a pre-Uber New York car service business asked users whether they had a positive or negative experience with the business. Those that clicked a button indicating they had a positive experience were redirected to a consumer review website, where they were offered a \$10 discount on a future ride to post a positive review. Those that clicked the button indicating they had a negative experience were redirected to the business' website where they could provide direct feedback to the company, and were not asked to write a review. As Deputy Bureau Chief Russell pointed out, incentivizing customers to provide favorable reviews without disclosing such payments is a form of false advertising and a deceptive trade practice that violates New York Executive Law § 63(12), New York General Business Law §§ 349 and 350, and the FTC Endorsement Guidelines.

In an era where consumers increasingly rely on consumer review sites, it is worrying to think that we may not be able to trust the authenticity of every review that we see—and, as companies adopt increasingly advanced techniques, we may not even be able to distinguish the genuine reviews from fake or paid ones. Thankfully, the AG's office is focused on this type of online consumer protection and continues to investigate such deceptive practices as a consumer protection measure.