Client Update
While You Were Celebrating: Cyber and Privacy News from the Holiday Season

NEW YORK
Jeremy Feigelson
jfeigelson@debevoise.com

Jim Pastore
jjpastore@debevoise.com

Lee Schneider
lschneider@debevoise.com

WASHINGTON, D.C.
Luke Dembosky
ldembosky@debevoise.com

Maryam Casbarro
mcasbarro@debevoise.com

FRANKFURT
Thomas Schürrle
tschuerrle@debevoise.com

SHANGHAI
Philip Rohlik
prohlik@debevoise.com

For our clients and friends who may have treated themselves to a holiday break from cyber and privacy news, here is a quick update on key developments.

UPDATED CYBER REGULATION FROM NEW YORK DFS

The New York Department of Financial Services issued an updated version of its draft cybersecurity regulation. Our detailed separate bulletin on this development is available here.

PRIVACY CONCERNS OVER UBER'S APP UPDATE

Senator Al Franken of Minnesota sent a letter to Uber raising privacy concerns about a recent update to the iPhone version of the Uber app. Among other changes, the update allows the continued collection of a rider's location information irrespective of whether the application is in use. Senator Franken urged Uber to "consider implementing in-app options that are distinct from operating-system level permissions;" to update its privacy policy to better describe its practices; and to provide an opportunity for "meaningful consent" for the recent changes by sending email and in-app notifications to users.

FINRA FINES 12 FIRMS $14.4 MILLION FOR INADEQUATE DATA SECURITY

The Financial Industry Regulatory Authority fined 12 firms a total of $14.4 million for allegedly failing to properly store electronic customer and firm data in accordance with applicable rules. Each of the settling firms were charged with deficiencies in their "write once, read many" storage format (WORM), which is supposed to prevent records from being altered, overwritten or erased. FINRA cited a variety of alleged failures, including improper retention of brokerage records and inadequate supervision of third-party vendors. WORM compliant storage of electronic records should assist in the event of a hack by preventing the hackers from changing official brokerage records.

ASHLEY MADISON SETTLEMENT

The parent company of Ashley Madison reached a $1.6 million settlement with the Federal Trade Commission (FTC) and state attorneys general over the site's well-publicized 2015 data breach. Notably, the FTC included Canadian and Australian privacy regulators in its press release and announced that it had exchanged information with them under the Safe Web Act, 15 U.S.C. §§ 41 et seq. The Safe Web Act allows the FTC to engage in cross-border information sharing with peer agencies in other countries that are investigating conduct under similar legal authority.

TURN INC. SETTLEMENT

The FTC announced a settlement on December 20, 2016 with digital marketing platform Turn Inc. The FTC alleged that Turn misled consumers by stating that consumers could disable Turn's tracking by blocking cookies, despite Turn using other methods, like web beacons, for tracking, and by representing that its opt-out mechanism would be effective in blocking targeted ads on websites and apps, when in fact the opt-out cookie only worked for mobile browsers. The settlement indicates an increasing degree of technical sophistication in the FTC's assessment of what makes a disclosure deceptive.

SEVENTH CIRCUIT APPLIES *SPOKEO* TO REJECT STANDING UNDER FACTA

In *Meyers v. Nicolet Restaurant of De Pere, LLC*, No. 16-2075 (7th Cir. Dec. 13, 2016), the Seventh Circuit dismissed a class action brought under the Fair and Accurate Credit Transactions Act, 15 U.S.C. § 1681 et seq. (FACTA). Plaintiff asserted that the defendant had given him a receipt containing his card's expiration date, which FACTA forbids. Interpreting the Supreme Court's recent decision in *Spokeo, Inc. v. Robins*, 136 S. Ct. 1540 (2016), the Seventh Circuit held that plaintiffs lacked Article III standing because a "violation of a statute that causes no harm does not trigger a federal case."

CHINESE CYBERSECURITY NATIONAL STANDARDS AND STRATEGY

China's National Information Security Standardization Technical Committee rolled out seven draft national standards that are intended—following a brief public comment period—to serve as nonbinding guidelines for the data privacy and security practices of companies operating in China. Subsequently, China's top internet regulator, the Cyberspace Administration of China, released a national cyberspace security strategy. It remains unclear whether these developments signal an increasing openness to Western business and technology, an intent to closely oversee them, or both. The strategy speaks of "opening up to the outside world, and safeguarding cybersecurity in an open

environment," but also of China's intention to "prevent product and service providers and other organizations from using their superiority in information technology to engage in improper competition or to harm users' interests."

EU REGULATORS ISSUE FIRST GUIDANCE ON CERTAIN GDPR CONCEPTS

With the effective date of the General Data Protection Regulation (GDPR) now less than 18 months away, the Article 29 Working Party—the official group of representatives of national data protection authorities within the European Union— issued its first, but still preliminary guidance on certain concepts of the new law. The guidelines and corresponding FAQs relate to (1) the "right to data portability," i.e., the data subject's right to request from the data controller its entire set of personal data in a commonly used format and to transfer the information to another data controller free of any impediments from the original controller, and (2) the requirement for certain companies to appoint a data protection officer (DPO). In addition, the authorities explain (3) the concept behind the "one-stop shop" supervision mechanism that will allow one national regulator to take the lead in supervising intra-EU cross-border data processing activity, or involving citizens of, more than one EU country. The guidance is open for stakeholder comments until the end of January 2017. The Working Party also advised about an upcoming GDPR guidance on Data Protection Impact Assessments, which are mandatory evaluation procedures to apply in cases of high-risk types of data processing in order to determine the impact on data protection rights, and the Certification for demonstrating GDPR-compliance.

* * *

Please do not hesitate to contact us with any questions.