Attorney Advertising

Robinson+Cole

Data Privacy + Cybersecurity Insider

Leveraging Knowledge to Manage Your Data Risks

CYBERSECURITY

Vevo Hacked through LinkedIn Message

Vevo announced this week that it experienced an intrusion into its servers by the hacking collective OurMine, self-described as a white hat organization that informs individuals and organizations of potential security vulnerabilities. When OurMine reached out to Vevo to inform it of a vulnerability, a Vevo employee dismissed the claim and told OurMine that they didn't have anything. As a result, OurMine published the data online before removing it after Vevo acknowledged that it had been compromised. The data included some sensitive information of individuals and companies using Vevo. 3.12 TB of Vevo's internal files was compromised and posted online. *Read more*

Offshore Cybersecurity Guidelines Issued

DNV GL recently issued a new, globally applicable recommended practice (DNLVGL-RP-G108) to assist oil and gas operators, system integrators and managers, and vendors in the offshore industry to manage increasing cybersecurity threats. The guidance is designed to help the oil and gas industry improve the security of its operational technology. *Read more*

INTERNATIONAL PRIVACY LAW

General Data Protection Regulation (GDPR) Series, Part 3 — GDPR Consent and Fair Processing

The General Data Protection Regulation (GDPR) (EU) 2016/679 of 27 April 2016, effective May 2018, will introduce major changes to the law on the processing of personal data in the European Union (EU). Over the next several months, several European Union (EU) law firms we work very closely with will join us in providing you with more information on the GDPR. Different themes will be tackled month by month to help you prepare for the GDPR deadline.

Part #3 of this GDPR Series is brought to you by the German law firm of Graf von Westphalen. Other blog entries in this series will be

September 21, 2017

FEATURED AUTHORS:

Conor O. Duffy
Linn Foster Freedman
Kathryn M. Rattigan

FEATURED TOPICS:

Cybersecurity
Drones
Enforcement + Litigation
International Privacy Laws
Privacy Tip

VISIT + SHARE:

Insider Blog
R+C website
Twitter
Facebook
LinkedIn

brought to you by the law firms of Mills & Reeve (UK), FIDAL (France) and VanBenthem & Keulen (Netherlands) as well as Robinson+Cole (United States). *Read more*

ENFORCEMENT + LITIGATION

Illinois Biometric Case against Shutterfly Survives

We have been following biometric cases in Illinois, including the case against Shutterfly [view related posts]. Late last week, an Illinois federal judge denied Shutterfly's motion to dismiss the case against it alleging that it violates the Illinois Biometric Information Privacy Act when collecting and storing face geometry scans through facial recognition software. In allowing the case to proceed, the judge rejected Shutterfly's argument that photographs are not included in the statutory definition of a biometric identifier, as that term applies to retina or iris scans, fingerprints, voiceprints, or scans of hand or face geometry and that the statute excludes information from writing samples, signatures, photographs, and tattoos. *Read more*

Supreme Court to Discuss Granting Review in Microsoft E-Mails Case on October 6

The U.S. Supreme Court recently indicated that it will consider the federal government's petition for a *writ of certiorari* in *United States v. Microsoft Corp.* at its conference scheduled for October 6, 2017. *United States v. Microsoft* is a "cutting edge" case that concerns the ability of law enforcement to obtain electronic documents stored abroad via a warrant issued under the Stored Communications Act of 1986 (SCA).

In 2016, a panel of the U.S. Court of Appeals for the Second Circuit unanimously quashed an SCA warrant issued to the Department of Justice that sought the contents of a Microsoft customer's emails stored on a server in Dublin, Ireland. In January 2017, the Second Circuit subsequently denied a request for an *en banc* rehearing (see our previous analysis of that decision here). In June 2017, the Office of the Solicitor General (OSG) filed a petition for a *writ of certiorari* with the Supreme Court requesting reversal of the Second Circuit's decision (see previous analysis here). *Read more*

DRONES

Advanced Weather Data: Vital for the Future of Commercial Drone Operations

Back in December 2016, Amazon executed its first customer delivery by drone in the United Kingdom. Now, as Amazon and other large

retailers aim for widespread deployment of drones for the delivery of goods to consumers, it is increasingly clear that advanced weather data is vital for ensuring that these delivery drones can fly weather-sensitive missions safely and efficiently. Weather is just one of the challenges commercial drones face. They also face things like birds and other drones, which require advanced navigation systems and a lot of coordination. The Federal Aviation Administration (FAA) estimates the number of commercial drones will reach 1.6 million by 2021. Weather data will in many ways dictate the speed and scope of commercial drone deployment. Advanced weather data can be leveraged for commercial drone operations for pre-flight planning, in-flight operations, and post-flight analysis. *Read more*

PRIVACY TIP #106

Online Romance Scams

I haven't been in the dating scene for decades, but I know it sure has changed. Millions of people participate in online dating, and I even know several couples who have found their significant other using online dating platforms. That's the good news. The bad news is that the Internet can be used for bad intentions, so protecting your privacy and practicing safe online behavior when seeking romance is really important.

The FBI reports that romance scams account for the highest financial losses of all Internet-Facilitated crimes. That statistic really surprised me. The FBI's Internet Crime Complaint Center (IC3) reported it received 15,000 romance scam complaints in 2016 — a 20 percent increase over the previous year. Losses suffered by victims exceeded $230 million, but the FBI says that estimate is low because only about 15 percent of these crimes are even being reported.

The most common states where victims live are California, Texas, Florida, New York, and Pennsylvania. In Texas last year, the IC3 received more than 1,000 complaints from victims reporting more than $16 million in losses related to romance scams.

How are all these people getting scammed?

The victims tend to be older widowed or divorced women whom organized crime figures and scammers target online. The victim may be active on Facebook, and in one case, the scammer reached out saying he was a friend of a friend. He started "liking" her posts on her wall and that turned into emailing back and forth. He posed as a construction executive who was working on a job in a foreign country, so they were unable to meet in person until a later time. Well, that later time never happened, and in the meantime, he got into an emergency and asked her to send him money. Because she was in love with him, she sent the money. Lots of it. How embarrassing.

According to the *Huffington Post*, victims who suffer romance scams are financially and psychologically "so embarrassed that they're reluctant to come forward even whenthey realize they've been scammed." It is such a problem that datingnmore.com even operates

a romance scam database that lists scams and alerts victims.

This week, the U.S. Attorney's Office in the Southern District of New York was successful in prosecuting an online romance scammer who posed as a millionaire and induced people online to give him personal financial information and steal their identities. He stole hundreds of thousands of dollars from his victims. According to prosecutors, he "promised business opportunities and romantic relationships just to steal his victims' identities and loot their bank accounts, then threatened those who discovered what he was doing."

His victims were a dozen women in cities including New York, Philadelphia, Chicago, and Atlanta. He met women on online dating platforms. Prosecutors have charged him with bank fraud, aggravated identity theft, and threatening interstate communications. He pleaded guilty to wire fraud and sending threatening communications.

The lesson here is to stay safe online. Be careful what you post to social media sites because scammers can and will use that information against you. Always use reputable websites but assume that con artists are trolling even the most reputable dating and social media sites.

If you develop a romantic relationship with someone you meet online, the FBI suggests that you consider the following:

- Research the person's photo and profile using online searches to see if the material has been used elsewhere.
- Go slow and ask lots of questions.
- Beware if the individual seems too perfect or quickly asks you to leave a dating service or Facebook to go "offline."
- Beware if the individual attempts to isolate you from friends and family or requests inappropriate photos or financial information that could later be used to extort you.
- Beware if the individual promises to meet in person but then always comes up with an excuse why he or she can't. If you haven't met the person after a few months, for whatever reason, you have good reason to be suspicious.
- Never send money to anyone you don't know personally.

If you suspect an online relationship is a scam, stop all contact immediately. And if you are the victim of a romance scam, file a complaint with the FBI's Internet Crime Complaint Center.