What’s trending on NP Privacy Partner

**FAA requires drone registration, workplace privacy issues proliferate,** EUA issues comprehensive regulation; courts address privacy cases naming parties by pseudonyms, Equifax FCRA class action settles, and student speech poses challenging First Amendment issues.

**Mobile Technology**

**FAA announces drone registration process**

With the holidays right around the corner, the U.S. Department of Transportation’s Federal Aviation Administration (FAA) this week announced its mandatory registration process for owners of small unmanned aircraft (UAS) or drones. The FAA chose this time because it “expect[s] hundreds of thousands of model unmanned aircraft will be purchased this holiday season,” said FAA Administrator Michael Huerta. “Registration gives us the opportunity to educate these new airspace users before they fly so they know the airspace rules and understand they are accountable to the public for flying responsibly.”

Drones have continuously been in the news from privacy concerns where drones are flown over private property to high profile crashes on the White House lawn and into the stands during a U.S. Open tennis match. Accordingly, the issue of when and where “pilots” may fly their drones has been a topic of increasing public, legislative and regulatory debate. The FAA’s biggest concerns are the numerous close calls of drones narrowly missing aircraft and the more than 600 drones reported in the vicinity of airports. The latter has led to the developing and testing of systems that can detect and intercept drones that fly within five miles of any airport. With the 2015 sales estimates indicating 1.6 million drones sold this year (and over 50% of them sold in the fourth quarter), the FAA decided to act in order to be able to identify every aircraft and to educate novices.

Registration begins on December 21, 2015, and is a statutory requirement applying to all aircraft weighing more than 0.55 pounds (250 grams) and less than 55 pounds (approx. 25 kilograms) including on-board attachments like cameras. In the spirit of the holiday season, and in an effort to encourage as many people as possible to register immediately, the $5 registration fee is waived for the first thirty days (from December 21, 2015, to January 20, 2016). Any owners of drones purchased after December 21 must register before their first outdoor flight.
Drone pilots may register either online or by mail. After completion, registrants will receive a Certificate of Aircraft Registration/Proof of Ownership that includes a unique identification number, which must then be marked on the aircraft. This identification number may be used on as many aircraft owned by each individual registrant.

Failure to register an aircraft may result in civil penalties up to $27,500 and in criminal penalties that include fines of up to $250,000 and/or imprisonment of up to three years.

With the explosion in the popularity of drones, we can and should expect much more public debate and subsequent legislation and regulation. In fact, the FAA pointed out that the new rule only applies to recreational use of drones and not to those used for business purposes, for instance.—Kevin Saunders

**Employee/Workplace Privacy**

*For employers: A friendly reminder that the Genetic Information Nondiscrimination Act generally prohibits inquiries regarding an applicant’s family medical history*

For employers with more than 15 employees, the Genetic Information Nondiscrimination Act (GINA) prohibits discrimination against employees and applicants on the basis of genetic information. The definition of “genetic information” includes information, among other areas, about an individual’s genetic tests, information about the genetic test of a family member and family medical history. An employer is generally prohibited from utilizing genetic information in making employment decisions, such as hiring, firing, advancement, compensation or other terms and conditions of employment. Except for some very narrow circumstances, GINA also prohibits employers from requesting, requiring or purchasing genetic information about applicants or employees.

In a lawsuit filed this month by the Equal Employment Opportunity Commission (EEOC), an employer’s practices and procedures relating to the collection of family medical history are under scrutiny. In EEOC v. Joy Global Underground Mining, LLC, 15-cv-01581, currently pending in the U.S. District Court for Western District of Pennsylvania, the EEOC contends that Joy Global Underground Mining, LLC (Joy), a company involved in the mining equipment manufacturing business, violated GINA when it required applicants provide, as part of the hiring process, information regarding family medical history. As set forth in the EEOC's complaint, after making a conditional offer of employment, Joy required applicants to state whether or not they had a family medical history for “TB, Cancer, Diabetes, Epilepsy, [and] Heart Disease” as part of its post-offer medical examination. The EEOC contends that this practice violates GINA because it “deprives applicants” from employment or “otherwise adversely affect[s] their status as applicants for employment because of their genetic information.” At this time, Joy has not yet responded to the complaint, so it is unclear whether it will be taking the position that its practices comply with GINA.

As noted above, while there are some exceptions to the general prohibition against acquiring genetic information in the employment context, they are extremely limited. Employers who request and/or consider genetic information or family medical history from employees or applicants should ensure that their practices comply with GINA.—Christopher G. Gegwich
In-house report confirms that employees are companies’ biggest threat to data security

Last week, the Association of Corporate Counsel (ACC) Foundation, which supports the efforts of the ACC, released a special study focused on the state of cybersecurity in the corporate sector, entitled “The State of Cybersecurity Report.” Over the course of approximately a month and a half, the Foundation collected more than 1,000 responses of members and non-members. Of these responders, 77% identified themselves as either general counsel or chief legal officers, plus an additional 14% who identified as assistant general counsel. This core group of in-house personnel shone a bright light on corporate data breaches, an issue that they identified was one of their greatest challenges. In fact, as the Report indicates, “data security is top of mind for in-house counsel” and noted a dramatic increase in budget allocation toward cybersecurity issues. In an age of ever-increasing security breaches, this may not come as much of a surprise that businesses are doubling down and spending their money on troubleshooting this problem. What may be surprising for some to learn is that the external threats are not the largest problem. Rather, this corporate group identified employee error as the number one cited cause of data privacy breaches. In fact, nearly a quarter of all security breaches can be traced back to employee error of some kind.

While this may be an astonishing finding to some, commentators have noted this theory with increasing frequency of late. And while it may seem like bad news to some, it’s actually promising. What this data tells us is that businesses need not sit back and wait for their systems to be infiltrated before acting. If businesses take the time to create and enforce policies and actually train their employees to appropriately prevent and react to breaches, companies might just be able to thwart these attacks in the future. One individual, highlighted in the Report’s Key Findings stated, “I wish we had done a better job at educating employees on cybersecurity issues, how to recognize and what to do and to become more informed on various ways that data breaches occur and proactive ways that could eliminate or reduce exposure.” Data breaches should no longer be deemed “the inevitable.” Organizations should be proactive. And by proactive, we mean really proactive. Simply issuing a one-time policy that is going to protect employers from these threats is not enough. Rather, businesses must engage in ongoing training and continually check in with their personnel to determine whether there is a gap—and the size of that gap—between understanding the hypothetical and practically knowing what to do as information crosses employees’ desks, computers and smartphones on a daily basis.

The Report cited that among the companies that have already experienced a data breach, 74% say that their company is making at least some change to their security policies, while only 58% reported making moderate to significant changes in response to a breach. Employers should be part of the latter group so that they are able to identify and recognize their weaknesses before they fall victim to what should no longer be seen as the inevitable.—Jessica Schachter Jewell

International

EU settles on stiffer data protection rules, steep fines for noncompliance

On December 15, 2015, the 28 member countries encompassing the European Union (EU) agreed on the General Data Protection Regulations (the “GDPR”) that will give consumers more control over how their data is used and retained. The new data protection rules mark some of the biggest changes to privacy laws in the EU in over two decades.
Under the GDPR, companies face tighter restrictions of the reuse of personal information, as companies must get an individual’s explicit consent to use their data. The GDPR provides individuals with the right to have any personal information corrected or removed if it is inaccurate under the regulation’s “right to be forgotten” provision. The new regulation also tightens breach notification requirements: companies must report any data breach that occurs within 72 hours.

Companies failing to meet the new rules could be responsible for paying fines of up to four percent of their total global sales. The new rules also increase liability for companies. Under the old rules, the data controller is only liable for data breaches in the EU; under the new rules, both the controller and the data processors will now be jointly liable for any damages associated with the breach, increasing liability for firms that perform outsourcing services for companies.

Establishing the new rules has been an arduous process. The revised data protection rules have been a work in progress since 2011, but have stalled due to disagreements among the European Parliament and Council regarding key issues. Although the new rules provide consumer groups with the enforcement mechanisms needed to force companies to comply with the new rules, the scope of penalties has left many companies feeling the fines are much too draconian.

The GDPR provisions will not take effect until 2018, and are subject to final endorsement by the European Parliament and the Council.—Gretchen E. Harper

**Privacy Litigation and Class Action**

**Court refuses to allow Ashley Madison customer to sue as a “John Doe”**

Customers of the Ashley Madison website frequented the company’s self-described “world’s leading married service for discreet encounters.” With the hacking of the website this past summer, personal information was stolen, which risked the public exposure and embarrassment of the site’s users. A plaintiff filed a putative class action suit as a “John Doe” plaintiff against Ashley Madison defendants in the United States District Court for the Eastern District of Arkansas. The plaintiff alleges that the Ashley Madison defendants were negligent in storing personal information and were unjustly enriched when they charged customers for a “paid-delete” service (which allegedly deleted a customer’s personal information for an extra fee, but did not delete the information). The Ashley Madison defendants moved to dismiss the litigation because the plaintiff relied upon a pseudonym rather than his name. The court agreed that the lawsuit may proceed only if the plaintiff files an amended complaint in his name. *John Doe v. Avid Life Media, Inc.*, No. 4:15-CV-640-JM (E.D. Ark. December 14, 2015).

The plaintiff sought to proceed anonymously to avoid exposing his “sexual habits [to] public scrutiny.” Rejecting this contention, the court held that the lawsuit reveals only that at one time the plaintiff was a member of a website that catered to individuals who wished to have “discreet relationships.” The court concluded that the details beyond the plaintiff’s signing up for the site are not relevant to the breach claims in his complaint, which means that there will be no revelation of his sexual proclivities. The plaintiff’s privacy concerns do not outweigh the strong presumption of open judicial proceedings under the Constitution and Federal Rules of Civil Procedure, which typically require parties to proceed under their own names except in very limited circumstances. As the court held, “[p]ublic access to this information [a party’s identity] is more than a customary procedural formality; First Amendment guarantees are implicated when a court decides to restrict public scrutiny of judicial proceedings.”—Steven M. Richard
**Settlement reached in Equifax FCRA class action**

Last week, plaintiffs in a Fair Credit Reporting Act class action against Equifax Information Services, LLC sought preliminary approval from a Virginia federal court of a settlement reached by the parties.

The foundation of the plaintiffs’ claims involves alleged incorrect reporting of Virginia state court judgments against individuals. Specifically, that, in its consumer reports, Equifax lists judgments as unpaid, even though its records do not contain information on the current status of those judgments. The plaintiffs claim that this is in violation of a credit reporting agency’s duty to follow reasonable procedures to assure maximum possible accuracy of information contained in a report.

According to the motion, the parties have litigated for over five years (one of the two cases was initially filed in 2010, and one was filed just this year), stretching through discovery and into “extensive motion practice,” including class certification. The parties entered into mediation, which reportedly ended in the proffered settlement.

Under the settlement, Equifax will pay $3 million into a settlement fund for class members “who are most likely to have suffered credit injury,” remove Virginia General District Courts judgments from the credit files of all persons (class members or not) for a period of no less than five years and provide to all class members four years of Equifax’s credit monitoring services or $180 in cash. Any class members who believe they suffered actual damages as the result of an inaccurate report containing a Virginia General District Court judgment can reserve claims for those actual damages.

Up next, court approval for the proposed settlement, which those involved in consumer FCRA actions claim has set the bar for such settlements.—Kate A.F. Martinez

**Eighth Circuit affirms denial of attorneys’ fees demand in copyright lawsuit against Doe defendants who were identified by IP addresses**

Leaverton was named specifically in the lawsuit. She denied downloading the film, and Killer Joe Nevada sought to dismiss its complaint against her. Before the Northern District of Iowa Federal District Court, she contended that she should be awarded attorney’s fees as the prevailing party in the copyright lawsuit, but the court declined to grant her request. On appeal, the Eighth Circuit found that Killer Joe had justifiable reasons for filing its lawsuit and upheld the denial of the attorneys’ fee demand. *Killer Joe Nevada LLC v. Doe*, No. 14-3274 (8th Cir. Dec. 4, 2015).

The Eighth Circuit rejected Leaverton’s argument that it is unreasonable for a Copyright Act plaintiff to sue a subscriber without first investigating whether the subscriber was responsible for the infringement. In a matter of first impression, the Eighth Circuit held that a plaintiff may properly sue a “John Doe” defendant to ascertain identity of the ISP subscriber. The appellate court also upheld that lower court’s determination that Killer Joe Nevada did not act with improper motivations, as the copyright holder promptly dismissed its lawsuit against Leaverton once it confirmed that she was not an infringer.

The litigation is another example where plaintiffs bring suit not knowing precisely who may be behind alleged activities on the Internet. Increasingly, lawsuits are filed against Doe defendants and discovery promptly ensues to try to determine who engaged in the Internet activity.
Depending on the context and circumstances, courts have reached varying conclusions on the propriety of such suits and the extent to which discovery may be served to try to identify an individual specifically.—Steven M. Richard

Social Media

Where does the schoolhouse gate end with student online speech?

As students communicate via social media and text messages, vexing issues arise when school administrators seek to discipline a student for speech. The controlling standard in the free speech analysis derives from a 1969 student speech case decided by the United States Supreme Court in Tinker v. Des Moines Independent School District, 393 U.S. 503 (1969), where the Court ruled that students do not “shed their constitutional right to freedom of speech or expression at the schoolhouse gate.” Under Tinker, in order for school officials to justify regulating otherwise-protected on-campus speech, officials “must be able to show that [the school’s regulatory] action was caused by something more than a mere desire to avoid the discomfort and unpleasantness that always accompany an unpopular viewpoint.” Where there is no showing that the student’s conduct would “materially and substantially interfere” with the requirements of appropriate discipline in the operation of the school, the prohibition cannot be sustained. Schools and courts are applying the Tinker analysis to off-campus speech (predominantly social media posts) outside of school hours.

Recently, a $425,000 settlement was announced in a Minnesota federal court lawsuit brought by a suspended high school student who contended that a school district violated his First Amendment rights relating to a two-word tweet. The student visited an anonymous website titled “Roger confessions,” where someone posted anonymously the following question: “did [the student] actually make out with [a female teacher at the student’s high school]?” The student did not create or maintain the website, and he responded to the question by posting “actually yes.” School administrators were not pleased with this post, which the student alleged to have made in jest. Faced with threats of criminal prosecution and expulsion, the student and his family agreed to a withdrawal agreement, which they claim was presented to them in duress. The student sued alleging violations of his First Amendment rights. The school district sought unsuccessfully to have the case dismissed as a justified exercise of its disciplinary authority. A Minnesota federal judge concluded that the student had adequately pled a claim. The judge ruled that the school district had not shown as a matter of law that his speech had caused a substantial disruption, was obscene, was lewd or vulgar or was harassing. This ruling allowed the case to proceed and prompted the recent settlement netting the student a significant payment, albeit without any admission of liability by the school district.

On the other hand, the United States Court of Appeals for the Fifth Circuit recently issued an en banc (full appellate panel) ruling, addressing the issues of off-campus student free speech in 101 pages of legal analysis explaining the court’s varying positions in its 12–4 vote. The majority upheld a lower court’s ruling that a high school did not violate the First Amendment by suspending a teen student who appeared to threaten two teachers in his rap recording posted on his Facebook page. A dissenting opinion warns that the “majority opinion obliterates the historically significant distinction between the household and the schoolyard by permitting a school policy to supplant parental authority over the propriety of a child’s expressive activities on the Internet outside of school, expanding schools’ censorial authority from the campus and the teacher’s classroom to the home and the child’s bedroom.” The student has filed a petition seeking that the United States
Supreme Court hear his case, and it may be a ripe time for the Court to consider Tinker’s applicability in an age of student speech occurring off-campus through the Internet.—Steven M. Richard

For more information, please contact:

— Christopher G. Gegwich at cgegwich@nixonpeabody.com or 516-832-7606
— Gretchen E. Harper at geharper@nixonpeabody.com or 312-977-4143
— Jessica Schachter Jewell at jsjewell@nixonpeabody.com or 401-454-1046
— Kate A.F. Martinez at kmartinez@nixonpeabody.com or 585-263-1332
— Steven M. Richard at srichard@nixonpeabody.com or 401-454-1020
— Kevin T. Saunders at ksaunders@nixonpeabody.com or 585-263-1561

NP PRIVACY PARTNER BLOG

Staying ahead in a data-driven world: insights from our Data Privacy & Security team.