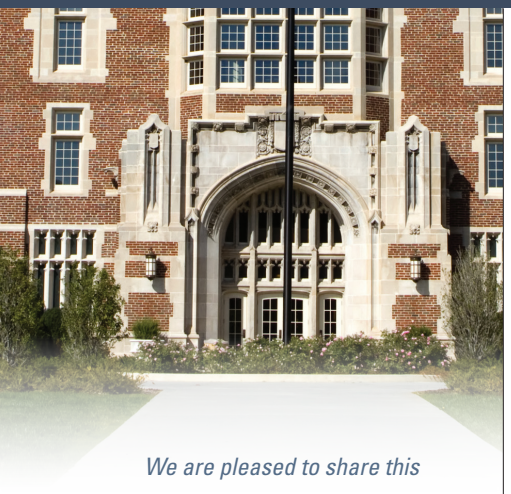
WIGGIN AND DANA *A Newsletter from the Education Practice Group*

# HIGHER ED LEGAL UPDATE

MARCH 2015



*We are pleased to share this first issue of the Wiggin and Dana Education Practice Group newsletter on matters of interest to the higher education community.*

*Our group has represented institutions of higher education for more than half a century on issues ranging from intellectual property to Title IX compliance, from labor and employment to data privacy. We will circulate our newsletter periodically to provide updates and articles on topics of concern to you.*

*We welcome your comments and suggestions.*

*Group Chair*

AARON S. BAYER

## COURSES



## Droning On:

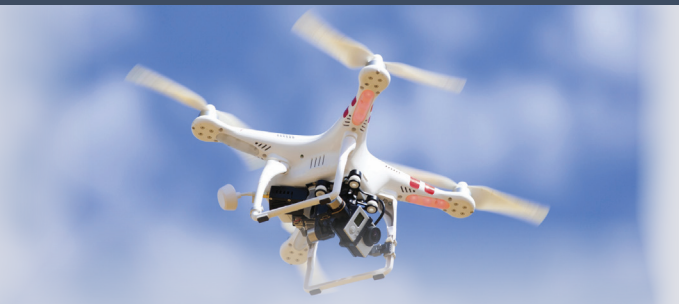
### A Primer on FAA Regulation of UASs

*David L. Hall and Benjamin M. Daniels, Wiggin and Dana LLP*

Colleges and universities across America have recognized that unmanned aerial vehicles (UASs) – also known as drones -- have broad academic applications. Indeed, the Federal Aviation Administration reports that of the 900 pending applications for exemptions to fly drones, 25 percent have come from private and public universities. For example, the University of Colorado at Boulder seeks to use drones to study tornadoes and supercells, in order to reduce the risk to weather researchers and storm chasers. The University of Florida has collaborated with the Florida Cooperative Fish and Wildlife Research Unit and the U.S. Army Corps of Engineers to develop affordable and user-friendly UASs for natural resource assessments and monitoring. Researchers at Central Michigan University use drones to study wetlands. In fact, dozens of colleges now offer courses in unmanned aerial systems, and Kansas State University offers a bachelor's degree in unmanned

CONTINUED ON NEXT PAGE

## Droning On: CONTINUED



aircraft systems, teaching students how to build and fly UASs.

Institutions of higher education have recognized not only the research capabilities of the UASs, but also the broader economic impact of UAS technology. Recent studies indicate that more than 23,000 jobs in unmanned aircraft systems could be created over the next 15 years. The possible applications are wide ranging, including insurance adjusting, geologic research, oil exploration, real estate listings, photography, surveying, and natural disaster preparedness.

**1. FAA Regulation and Oversight**

The FAA's oversight of UAS use by private institutions presents significant challenges. The Federal Aviation Administration Modernization and Reform Act of 2012 ("Reform Act") requires the FAA to develop a regulatory system for UAS use. The FAA is to design a system for granting Special Airworthiness Certification; that is, a process for approving the use of certain UAS designs and safety equipment, and standards for UAS pilot training programs and commercial UAS operation. This system was supposed to be in place in 2015, but the FAA recently announced that it would not issue regulations until 2017.

Its delay in implementing the Reform Act has not stopped the FAA from regulating the commercial use of UASs. Last June, the FAA issued an interpretation of the Reform Act that essentially banned the commercial use of UASs. The FAA emphasized the general prohibition against commercial use while allowing general recreational use by hobbyists (with certain limitations).

**2. Research Institutions Push Back**

This caused an outcry from research institutions. Although it is not settled whether the FAA's ban on commercial use applies to private universities, professors from sixteen elite research institutions signed a letter to the FAA decrying the expansion of FAA jurisdiction, the unreasonable definition of aircraft adopted by the FAA, and the unwarranted distinction between recreational and commercial UAS use. The professors noted that UASs are uniquely able to contribute "to environmental science, GIS mapping, filmmaking, archaeology, agriculture science and many other fields." Particularly distressing was the idea that "a ten-year-old hobbyist can freely fly model aircraft for recreation, while our nation's scientists, engineers, and entrepreneurs are prohibited from using the same technology in the same types of environments." Soon thereafter, the Council on Governmental Relations (an organization that represents 188 research universities) filed suit challenging the FAA's interpretation in federal court. While this lawsuit wends its way through the court system, however, the broad ban remains in place.

**3. FAA Exemptions Available**

There is one work-around: the FAA has implemented an interim policy that allows commercial operators to apply for an exemption pursuant to Section 333 of the Reform Act. In making this determination, the FAA must assess whether the UAS will endanger the public or threaten national security. This requires the FAA to evaluate (1) the UAS's size, weight, speed, and operational capability; (2) whether the UAS will be operated in close proximity to airports and populated areas; and (3) whether the UAS will be operated within visual line of sight of the operator. See Section 333(a)(1). If it concludes that the UAS poses no hazard, the FAA can issue an exemption permitting specified commercial use without an airworthiness certificate.

To date, the FAA has granted nearly twenty exemptions in a variety of industries. Most recently, the FAA granted exemptions to companies to conduct flare stack inspections, aerial photography and surveys, and film and television production. Other exemptions allow companies to perform operations for aerial surveying, construction site monitoring, and commercial movie production.

This process gives institutions of higher learning the option of pursuing an FAA exemption under Section 333. This is not a trivial process: the Section 333 application must describe the nature of the exemption sought, explain why granting the exemption would be in the public interest, and supply a summary that the FAA will publish in the Federal Register. The FAA then allows public comment on the petition. The process can take months.

In addition, schools can apply for experimental certificates to test new UAS design concepts, new equipment, new UAS installations, new operating techniques, or new uses. Schools must submit an application, and the FAA will conduct safety evaluations and inspections to verify proper completion of the certification procedures.

Institutions of higher education should consider these options with the advice of counsel.

# Mitigating Cybersecurity Risk

*Michael T. McGinley, Wiggin and Dana LLP*

At the end of the year, Sony Pictures Entertainment shot into headlines when hackers broke into Sony's network, stole sensitive data and intellectual property, and famously publicized its executives' salacious emails. The incident triggered a wave of nervous cybersecurity program reviews in corporate boardrooms nationwide, but the lessons from Sony's misfortune are applicable to institutions of higher education as well. They face significant cyber risk and would be wise to use the Sony incident to help frame their own internal cyber-risk assessments.

In 2014 alone, data breaches at UC Berkeley, the University of Maryland, the University of Indiana, and the University of Delaware accounted for the exposure of over half a million records. These were just a few of the many data breaches that higher educational institutions across the country reported last year, and an increase in reported breaches in 2015 can be expected based on the proliferation of online data, digital devices, and the growing sophistication of hackers.

Educational institutions make good targets because of the large volume of sensitive information they acquire, develop, and maintain on their networks – from student identity numbers and health records to credit card and financial information of applicants and their parents. Institutions also maintain highly sensitive research and development data in which the institution and faculty members may have significant intellectual property interests.

This makes schools prime targets for hackers seeking to harass, embarrass, or profit from information they can access. Schools also may be targeted by foreign intelligence organizations seeking to uncover cutting-edge technology developed by an institution's researchers or foreign governments seeking to punish a school for permitting the broadcast of a particular viewpoint (or an unpopular movie).

Keeping sensitive information private and secure against these adversaries is no easy task, even for well-funded universities. Schools can mitigate their cyber risk through proactive management activities, including the following:

1. **Apply the Cybersecurity Framework.** Managing cybersecurity risk in academic institutions is complicated. One tool to which schools can turn for help is the Cybersecurity Framework, published in 2014 by the National Institute for Standards and Technology ("NIST"). Although the Framework was designed originally to improve the cybersecurity of the nation's critical infrastructure, its universal, cross-industry format makes it surprisingly beneficial to educational institutions. The Framework applies equally to academic organizations of any size and level of cybersecurity sophistication.

   The Framework outlines a structured approach for evaluating cybersecurity preparedness and managing cybersecurity risk. It complements an institution's existing risk management program by providing a taxonomy to help the institution identify its current cybersecurity posture and to assess its progress toward its cybersecurity goals.

   For example, the Framework identifies the need to protect data as a core cybersecurity activity, breaks down and analyzes the steps involved in protecting an institution's data – controlling access to data, training employees who have access to sensitive data, and designing and implementing, and implementing specific measures to make stored data more secure. Using this approach, schools can make more informed cost-benefit assessments with respect to each step and gain a better understanding of their current capabilities, shortfalls, and the risks associated with different courses of action.

2. **Know the limits of your cyber insurance.** According to Sony CEO Michael Lynton, Sony's insurance will completely cover the costs associated with the attack on his company, which analysts have estimated could reach $100 million. Recent litigation suggests that courts are increasingly unlikely to find that commercial general liability ("CGL") policy coverage encompasses a cybersecurity incident. It is essential for schools to review the scope of coverage and liability limits of their existing policies to ensure they have adequate cybersecurity coverage. Issues include whether the insurer or the policyholder has authority to decide what lawyer and other professional to hire once a claim is made and whether the costs of defense are in addition to or erode your policy limits. The cyber insurance market is seeing double-digit growth and delivering products specifically tailored to the education sector, but cyber policies are still relatively new and there is no standardized form used by all insurance companies. Risk managers should

CONTINUED ON NEXT PAGE

## A Lesson in Cybersecurity CONTINUED

carefully compare the specific terms in the policies being offered by different insurers.

3. **Actively manage your third-party cyber risk.** Educational institutions engage countless vendors to perform a host of daily functions, often in roles that permit them access to sensitive data. Failing to account for these vendors in an institution's cybersecurity preparedness can be disastrous. For example, the massive data breach at Target stores resulted from the retailer's failure to ensure its HVAC vendor was practicing good cyber security. Criminals were able to exploit a hole in the vendor's security and tunnel directly into Target's network. Schools should evaluate each vendor's cyber hygiene practices—particularly if a vendor has access to the school's network or handles personally identifiable information of staff or students. To get a sense of their vendors' cyber preparedness, schools should ask to review each vendor's incident response plan, cybersecurity audits, and staff cybersecurity training records. Furthermore, schools should review with legal counsel every vendor contract to make sure it includes provisions requiring encryption of sensitive data, compliance with applicable privacy laws, and indemnification provisions that allocate responsibility should a cyber event occur. Each contract also should require a vendor to carry a defined minimum amount of cyber insurance.

# A Few Things Universities Should Remember for Employment-Related Immigration & Compliance

*Najia Khalid, Wggin and Dana LLP*

Institutions of higher education have double responsibility when it comes to employment-related immigration and compliance, as visa matters for both international students and international faculty members/employees must be carefully managed. It is, therefore, essential for University in-house legal and human resources teams to be familiar with common F-1 student visa matters, basic employment-based visa matters, and the general transition process from student visa status to employment-based visa status.

Here are a few things to remember regarding employment-related immigration and compliance issues that arise with colleges and universities.

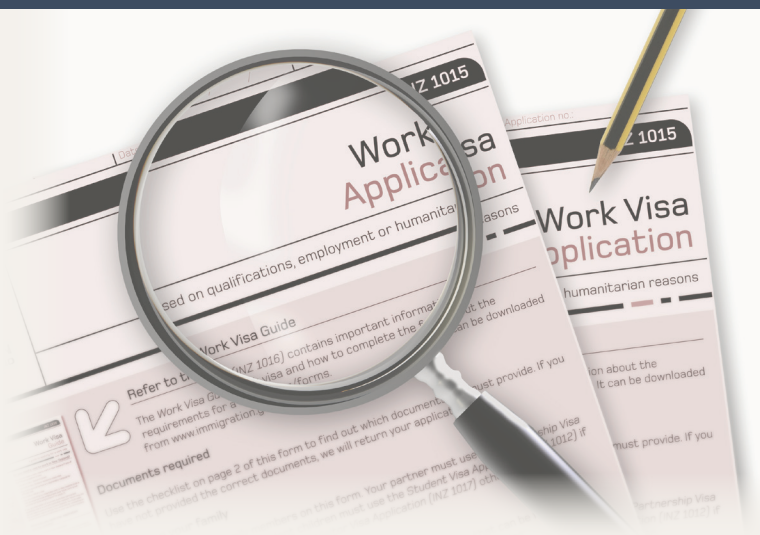
For F-1 visa students, Optional Practical Training (OPT) requirements for students in Curricular Practical Training (CPT), pre- and post-completion OPT, and Science, Technology, Engineering, and Mathematics (STEM) should be carefully reviewed before students engage in any work activity. They must continue to be monitored until the approved activity is completed. Employment questions often arise with respect to acceptable OPT work activities, OPT unemployment periods, and STEM extensions.

**1. There are different types of work activities authorized for OPT.** The institution must be attentive to the limitations and record-keeping requirements for each one.

- Paid employment for one employer, multiple employers, or an agency
- Short-term employment for performing artists (evidence of performances should be maintained)
- Work for hire or "1099 employment" where a service is performed based on a contractual relationship (evidence of contract duration and contractor should be maintained)

CONTINUED ON NEXT PAGE

## Immigration & Compliance CONTINUED




- Self-employment where students are business owners (evidence of full time employment, business license, and business activities should be maintained)
- Unpaid or volunteer work (cannot volunteer for a position for which others are usually paid, but may volunteer for a non-profit organization as long as the activity does not violate any labor laws)

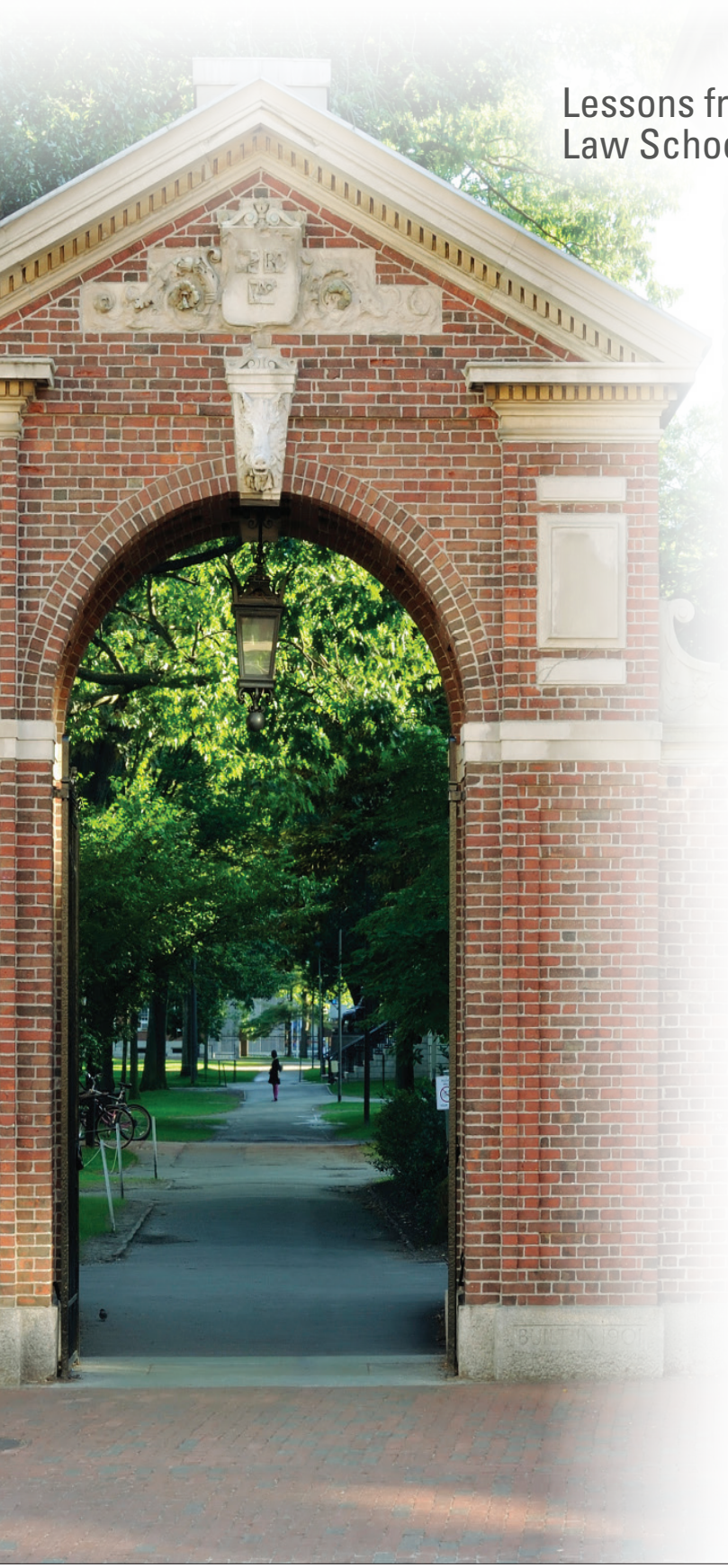
**2. Students on post-completion OPT are only allowed a total of 90 days of unemployment time.** This includes each day of not working during the OPT dates indicated on the EAD (Employment Authorization Document) card AND during the H-1B cap gap provision period. If the allowable period of unemployment is exceeded, then, even if the EAD card remains valid, it is considered a violation of F-1 status.

**3. STEM OPT extensions are only permitted for eligible students who are working for employers enrolled in the E-Verify database system, which is used to electronically verify the employment eligibility of newly-hired employees.** In a majority of states, system enrollment is voluntary (and many employers are not enrolled in E-Verify).

For faculty members/employees utilizing employment-based visas, the University should carefully review its visa sponsorship policy, understand the roles of the University as visa sponsor and its outside immigration counsel, carefully review visa terminology, procedures, and common visa categories, and be versed in I-9 compliance. Employment questions often arise with respect to visa ownership, payment of related fees, and termination of visa employment.

- Employment-based visas belong to the University, and the University should retain its own immigration counsel to prepare its visa petitions (as opposed to using counsel retained by the employee/faculty). The University has the discretion to initiate and withdraw employment-based visa processes. With this, visa status is never guaranteed, and, therefore, all job offers, including tenure-track positions, should be contingent on obtaining and maintaining valid work authorization. The University should have a standard policy outlining all related points.
- The University is required by law to pay for certain visa-related costs. Such costs, including H-1B fees and PERM legal fees/advertising costs, cannot be paid by, or charged back to, faculty members/employees.
- If the University terminates an H-1B worker before the visa petition expires, it must pay the cost of his/her one-way coach class return airfare to the last country of residence, and timely report the termination to the Immigration Service. The H-1B worker is obligated to leave the U.S. immediately (there is no grace period), or timely file for a change of visa status with the Immigration Service. Layoff situations should be carefully evaluated in advance.

The in-house legal and human resources team should conduct regular reviews of employment-related immigration and compliance matters, as they are often case-specific and affect more than just visas.



# Lessons from the OCR Investigation of Harvard Law School

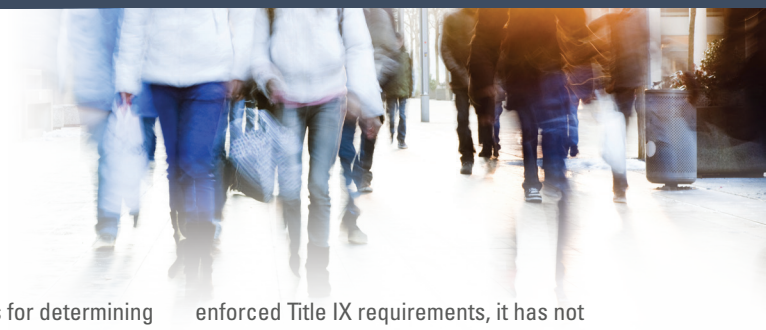
*Benjamin M. Daniels, Wiggin and Dana LLP*

Last year, a group of Harvard Law professors thrust the Law School into the forefront of the Title IX debate by publishing a letter criticizing a new University-wide policy against campus sexual assault. The University had adopted the new policy in July 2014, in response to the U.S. Department of Education, Office for Civil Rights' (OCR) investigation of Harvard College and Harvard Law School. Among other things, the new policy created a centralized office of trained investigators, mandated use of "preponderance of the evidence" standard, and gave complainants additional procedural rights. Interestingly, OCR did not have any input into the University-wide policy. Harvard had provided OCR with the policy for comment, but implemented the policy after the agency failed to comment after three months.

The new policy drew fire from 28 law school professors. In a letter published in the Boston Globe, the professors criticized the policy as "inconsistent with many of the most basic principles we teach" and "lack[ing] the most basic elements of fairness and due process." The professors complained that the accused could not get discovery, could not confront the witness, did not have the right to adequate representation, and faced a structurally biased investigation. The professors also criticized the policy's provisions regarding an impaired or incapacitated student's ability to consent due to drugs or alcohol. This "starkly one-sided" treatment of the complex issue, the professors claimed, reflected the University's decision "simply to defer to the demands of certain federal administrative officials." The Law School responded by adopting interim procedures that incorporated the University-wide policy, but also provided enhanced procedural protections for the accused. For example, accused students now have a right to a lawyer and access to need-based financial assistance to obtain a lawyer.

Meanwhile, Title IX advocates decried the University-wide policy's omission of an affirmative consent standard, contending that it is needed to replace the notion that the lack of "no" constitutes consent. California has already required use of the "yes-means-yes" standard, statutorily

CONTINUED ON NEXT PAGE



## Lessons from OCR CONTINUED

defining sexual consent between people as an affirmative, conscious and voluntary agreement to engage in sexual activity. The State University of New York system adopted a similar definition for all of its campuses. And Connecticut lawmakers recently introduced a bill that would require all public and private colleges in Connecticut to adopt an affirmative consent standard. In fact, Harvard is the only Ivy League school not to use the standard.

### OCR'S FINDINGS OF VIOLATIONS

In December, OCR found that the University-wide policy and the Law School's procedures violated Title IX. In an eighteen-page letter of findings, OCR first identified a number of deficiencies in the new University-wide policy. Among other things, the University-wide policy failed to cover off-campus incidents, improperly implied that the school might use mediation to resolve sexual assault cases, and implied that students could not simultaneously pursue criminal investigations and Title IX investigations. Finally, the policy did not adequately assure students that the complainant and respondent be given equal opportunity to participate in any appeals process. In an apparent response to the law professors, OCR required the University to "make clear that no School or unit-based policy, procedure or process can reverse or alter a factual finding, remedy, or other decision made through the University's Title IX Procedures."

OCR also found deficiencies in the Law School's procedures. The Law School procedures lacked an assurance that the parties had an equal opportunity to present witnesses, failed to indicate it would take steps to prevent recurrence, failed to include specific timeframes for determining sanctions, and failed to require the school to provide periodic status updates to both parties. The agency also noted that the School had not trained all decision makers in Title IX compliance. Finally, OCR found the Law School had violated Title IX by mishandling certain past complaints, noting that the Law School took over a year to make a decision in one case.

### LESSONS FROM OCR'S FINDINGS

Although OCR did not resolve the due process and affirmative consent issues, schools can draw a number of lessons from the OCR investigation of Harvard Law School.

1. For schools operating within a larger university, OCR tacitly endorsed Harvard's University-wide policy and made clear that decisions regarding sexual harassment should be made at a university level by independent investigators.

2. OCR has not been particularly responsive to concerns about the due process rights of the accused. This issue came to the forefront during the Law School investigation. Without addressing the law professors' critique, OCR left intact some of the Law School's enhanced procedural protections for the accused. OCR, though, largely took the matter out of the Law School's control by requiring that "no School or unit-based policy, procedure or process can reverse or alter a factual finding, remedy or other decision made through the University's Title IX Procedures."

3. OCR does not yet require schools to employ the affirmative consent standard. Although the Department has aggressively enforced Title IX requirements, it has not yet embraced this heightened standard. It is unlikely that a federal definition will be forthcoming soon—even the much lauded Campus Accountability and Safety Act that died in the Senate last year did not embrace that standard. States have nonetheless begun addressing the issue, with California and New York taking the lead. However, schools should note that, even in the absence of a federal or state mandate, schools increasingly have adopted the standard.

4. While OCR would often allow schools to agree to policy changes without any findings of violations, it has toughened its stance. Even if a school complies with OCR's recommendations and adopts compliant policies and procedures, the agency still tries to find past violations of Title IX. Strategically, therefore, a school under investigation may be better off trying to avoid a finding that it is currently violating Title IX by making sure, in consultation with OCR, that its current policies and procedures are compliant. It can then try to minimize the scope of any findings of past violations, understanding that it will be hard to avoid them entirely. Princeton University recently used this strategy effectively. The Law School did it less effectively; the University failed to obtain prior OCR approval of the University-wide policy and the Law School failed to get prior approval of its procedures. As a result, OCR found that both are currently violating Title IX.

Given the complex and continually evolving OCR enforcement scheme and state regulatory requirements, institutions of higher education should periodically revisit their Title IX policies and procedures with counsel.

**Wiggin and Dana Education Practice Group**

Our Education Practice Group has long-standing relationships with colleges and universities, and independent and proprietary schools, as well as extensive experience counseling them on the full range of legal issues they face. Our lawyers work closely with boards of trustees, presidents, senior administrators, deans, department chairs, and in-house counsel to find practical solutions to complex legal issues.

*For more information, please see the full Education Practice Group description at* **www.wiggin.com/education-law** *or contact:*

AARON S. BAYER
860.297.3759
abayer@wiggin.com

**About Wiggin and Dana LLP**

Wiggin and Dana is a full service firm with more than 150 attorneys serving clients domestically and abroad from offices in Connecticut, New York and Philadelphia. For more information on the firm, visit our website at www.wiggin.com.

# UpcomingEVENTS

## Privacy & Security of Personal & Healthcare Information in the Workplace

Labor and Employment attorney **Joshua Walls** and Cybersecurity and Privacy attorneys **Michelle DeBarge** and **Michael McGinley** will address timely topics in our New Haven and Stamford offices, which will:

- Help you identify the types of sensitive information your company maintains, and where you maintain it;
- Address the policies and procedures you must have in place to comply with state and federal law;
- Analyze when HIPAA does and does not apply to medical information collected in the employment context (e.g., information collected for FMLA leave, ADA accommodation requests, workers' compensation claims, and health benefits administration); and
- Provide critical guidance on training and educating your workforce so you can avoid unnecessary exposure.

This program will be beneficial to human resource professionals, health benefit administrators, in-house counsel, information security officers, and anyone who manages or supervises employees. The event will be held on March 18th in New Haven and on March 25th in Stamford.

## Columbia University Start-Up Seminar

Wiggin and Dana attorney **Najia S. Khalid** will be presenting a seminar for faculty and students at Columbia University on April 13th. The seminar will review common visa issues faced by entrepreneurs, startups and international students.

## University of New Haven's Spring OPT Information Sessions

**Najia Khalid** will be speaking at the University of New Haven's Spring OPT Information Sessions for F-1 Students. She will provide international students with information about working in the U.S. after graduation.

## 6th Annual Connecticut Privacy Forum

On April 23rd in New Haven, Wiggin and Dana will host the 6th Annual CT Privacy Forum.

Panels and presentations will address:

- the cyber threat environment for 2015;
- emerging standards for 'reasonable' enterprise cybersecurity;
- key takeaways from recent case law and regulatory enforcement actions;
- optimizing cyber liability insurance coverage; and
- understanding compliance and liability risks in leveraging 'big data' and entering the market for the 'Internet of things.'

*For more information on any of our upcoming events, please contact marketing@wiggin.com*

## COMING IN THE NEXT HIGHER ED LEGAL UPDATE

- **When a parent's bankruptcy filing may require a college to refund tuition payments**
- **How a university's activities at home and overseas can unexpectedly implicate federal export controls – traps to avoid**