

# Law360

May 3, 2013

## **Q&A With Hunton & Williams' John Delionado**

John J. Delionado is a partner in Hunton & Williams LLP's Miami and Washington, D.C., offices. He defends businesses and individuals investigated by the government and on cybersecurity and privacy matters. He regularly represents companies in complex regulatory enforcement matters and class actions, and has led investigations into cyber intrusions, cyber extortions, and computer breaches for Fortune 500 and multinational companies, including investigations into two of the largest credit card hacking events in retail history. Prior to joining Hunton & Williams, he was an assistant U.S. attorney for the Southern District of Florida.

### **Q: What is the most challenging case you have worked on and what made it challenging?**

A: While I was an assistant U.S. attorney, I served as lead prosecutor on *U.S. v. Morales et al.* — the first U.S. trial involving the hijacking of a commercial plane since 9/11. In 2003, six men, some armed with knives, hijacked a Cuban state airliner taking off from Cuba and heading to Miami. The U.S. Air Force brought in fighter jets to intercept the plane before it reached Florida and escort it to Key West, where the suspects surrendered. The trial was very intense, particularly given that the memories of 9/11 were still so fresh in everyone's minds. We were not even sure that we would have all our witnesses as some had returned to Cuba and might not have been allowed to return for trial testimony.

It was one of my first high-profile cases as an AUSA and to make it even more challenging, the Cuban papers were laying the ground work to criticize the U.S. in case we lost by suggesting that my wife, a Cuban-American who was also an AUSA at the time, was part of the anti-Castro "Miami Mafia." The prosecution was successful and we were able to win convictions and sentences of more than 20 years for all six hijackers. Most importantly, it helped to cease a wave of violent takeovers of planes and boats by individuals in Cuba that put innocent people at risk.

### **Q: What aspects of your practice area are in need of reform and why?**

A: The Electronic Communications Privacy Act, which governs real-time wire interceptions and stored messages, is in great need of reform. When it was first introduced no one envisioned the way we would communicate today. The amendments have not come rapidly enough and it is now out of date with the ways people share, store, and use media today. There is a real lack of clarity and, as is the case, whenever you try to put a round peg in a square hole, inconsistency in the way the act gets interpreted.

As more personal and business computing moves to the cloud, the incongruities will become more apparent and will affect criminal investigations, cybersecurity measures, and even advertising.

Since it was enacted, technology has advanced well beyond what was contemplated at the time. The act needs to be revamped with better definitions and clearer guidance about what conduct is illegal.

**Q: What is an important issue or case relevant to your practice area and why?**

A: My practice often involves issues of cybercrime and cybersecurity, and it is time for comprehensible legislation and regulatory standards. Despite the increasing sophistication and occurrence of cybercrime, there is a notable lack of consistent legislation and uniform standards. Companies are in an exceedingly vulnerable position because they are under attack like never before from nation-states, criminals, terrorists and insiders. Clear guidance from those who are in the best position to help companies turn back these threats will make the U.S. more secure.

The president's recent executive order is a step in the right direction that should be allowed to evolve. For instance, while the EO emphasizes voluntary information sharing between companies and the government regarding critical infrastructure, it is worded in terms of "consultation" and "voluntary" adoption of a yet-to-be-developed cybersecurity framework. One of the issues that my partners and I have written and spoken on at length, however, is the lack of liability protection leaving businesses vulnerable in civil court. Clearly it is time for legislation, or we may soon see a spate of litigation against companies that have received information about threats from the government but do not or cannot act on it because of technical limitations or a different view of the articulated threat.

**Q: Outside your own firm, name an attorney in your field who has impressed you and explain why.**

A: Doug Sandberg, senior vice president and general counsel at credit card-processing company WorldPay, is one of the most impressive attorneys I have worked with over the years. In 2008, RBS WorldPay (as it was called at the time) was targeted by a sophisticated group of criminals in Eastern Europe. The group stole nearly \$10 million from ATMs around the globe in a 24-hour period. The U.S. Department of Justice, in fact, called it "perhaps the most sophisticated and organized computer fraud attack [ever perpetrated]." While Doug hadn't had any experience with data breaches, he got a crash course in the issues, and was able to advise his company as well as the affiliates and parents in the U.S. and U.K. He managed the risks but did not lose sight of the fact that the only chance law enforcement had to catch the criminals was if he authorized his colleagues, attorneys and consultants to share information with law enforcement.

As a result of Doug's ability to manage the situation, there were successful prosecutions and the company was ultimately able to obtain criminal restitution — a very rare feat in an international hacking case. The company was ultimately lauded by the FBI for its level of cooperation — a direct reflection on Doug's efforts. While no company wants to face a breach of that magnitude, WorldPay was lucky to have Doug running point and I am glad to have had the opportunity to work with him.

**Q: What is a mistake you made early in your career and what did you learn from it?**

A: Early in my career when I was in the U.S. Attorney's Office, I had two big cases land on the same day. I had to argue before the Eleventh Circuit Court of Appeals in the morning and then had to shift gears, and pick a jury in district court in the afternoon. As anyone who has had an appellate argument knows, you have very little left in the tank after you are done. Being tired, I forgot this trial judge's rule that prosecutors could not ask anyone in the panel whether he or she

would convict if a certain set of facts were proven. The judge called it asking the “ultimate” question. I walked right into it and asked the juror the ultimate question. The sidebar that followed provided clear instruction that when you step into court you had better know the law, procedure, but also, the judge’s rules.