Portfolio Media. Inc. | 111 West 19th Street, 5th Floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

Coronavirus Q&A: MoFo's Global Privacy Group Co-Chair

By **Allison Grande**

Law360 (June 26, 2020, 8:33 PM EDT) -- In this edition of Coronavirus Q&A, Morrison & Foerster LLP partner Miriam H. Wugmeister digs into growing concerns among in-house counsel about the increased personal data they'll likely need to collect to safely reopen their businesses and how her homebound colleagues and clients are teaming up to fight hackers remotely.

Miriam H. Wugmeister

Wugmeister, co-chair of the firm's privacy and data security practice, has helped steer hundreds of clients through data security incidents and advises a wide range of companies on how to navigate the growing global patchwork of privacy and data protection laws in the U.S. and abroad.

The attorney, based in New York but working from her Connecticut home due to the COVID-19 pandemic, spoke with Law360 as part of a series of interviews with lawyers about how the crisis has impacted business and brought about a host of new legal questions and considerations.

As part of efforts to gauge how the pandemic has affected companies, MoFo recently surveyed more than 100 in-house general counsel, who ranked privacy and data security third and fourth, respectively, on their lists of the top legal risks that COVID-19 poses to their businesses as stay-at-home orders expire. The percentage of respondents flagging those issues has more than doubled since March, when the firm conducted its first impact survey.

This interview has been edited for length and clarity.

When MoFo surveyed general counsel in March for its first COVID-19 impact survey, 18% of respondents cited privacy and 29% named data security as a top legal risk. The numbers shot up to 59% for privacy and 50% for data security in the latest survey, released this month. What's contributed to this surge?

On the privacy side, I think the big change is with folks starting to think about return to work. There's a lot of pressure for employers to collect information that they don't really want, like temperatures, like answers to questionnaires, like contact tracing. So employers really don't have a need for that information, and from an employment law perspective and from a privacy law perspective, they don't really want it. Even though we've been talking about data minimization as privacy professionals for ages,

that doesn't necessarily roll off the tongue for every single employer. So I think that there's a lot of anxiety for employers that really want to do the right thing to protect their employees and protect their guests, but they don't really know what to do with all that data, how long to keep it, how to store it, who to give access to.

On the data security side, most companies went from some percentage working at home to everybody working from home in a blink of the eye. And of course, when that happens, things don't go perfectly. And the bad guys are totally taking advantage of the fact that IT departments are completely stretched. We all did this big transition so quickly, making our attack footprint so much bigger. And there's just a tremendous rise in the number of, for example, ransomware attacks; there's been an explosion. So you see on the data security side just a lot of nervousness that do you have the right resources, and a lot of companies have furloughed people so they don't necessarily have all their people they normally would to respond to various threats.

Back in March, privacy and data security issues weren't top of mind. It was how do we stay in business, how do we make sure we can pay people. And I just think it's changed, as companies have figured out that people can still do their work, now it's the other bigger picture stuff.

As you mentioned, the reopening process is underway in many places. How do you envision the back-to-work process going and what are the biggest privacy and data security risks facing companies as they get back to business?

Companies are going to want to be able to demonstrate that they are taking steps to protect their employees, so I do think there's going to be a combination of temperature checking and questionnaires and contact recording. What employers can do is, to the greatest extent possible, think very clearly about what you're going to do with the information once you collect it, and collect as little as possible.

So on the questionnaires, there's really four basic questions that most companies want to ask: Have you tested positive, have you been exposed to somebody who's tested positive, do you have any of the symptoms and do you have a temperature. And actually, you can just ask it as one question. You can say if any of the answers to the four questions is yes, don't come to the office. Why do you need to know yes or no for each one?

On the data security side, the biggest issue is, the bad guys are being more stealthy, but they also are looking for the easy targets. If you see an alert, raise your hand. A lot of companies now have great technology, and a lot of these systems send up alerts, but there may not be enough people to look at them, or they may not look at them fast enough. So one of the things companies can do is really try to make sure they're focusing on those alerts, because if you can essentially stop the bad guys before they get a good foothold in your system, they'll just move on to the next company.

How has the pandemic impacted your practice and your ability to help clients with their data security issues?

What's interesting is that people both within our firm and our clients have really adapted unbelievably well to doing things over videoconference. We've had three significant ransomware attacks in the last two weeks, and it used to be people would talk about, when they had some major crisis, they would set up what they called a war room, and everybody would be physically there. And guess what? You just do it over the phone and on video.

Same thing with tabletop exercises. Traditionally, you always try to do tabletop exercises by getting all the relevant people in the same room to the greatest extent possible. Guess what? I'm doing them virtually now. It takes a little bit more work, you have to draw people out a little bit more. But Zoom and [Microsoft] Teams and WebEx and all these different systems where you can actually see people really has made a huge difference in being able to read the room virtually. Because you can see who's the person who's looking quizzical, who's the person who looks like they might have something to say but just isn't ready to jump in.

Where it gets harder is if you're doing an investigation and you need to interview people. One of the things we do for our clients is we come in and look to see whether their privacy compliance program is where the company expects it should be. Is it easier to do those assessments in person? Sure. Can you do them by phone or video? Yes. And as for the cybersecurity firms of the world, they all now have [this technology] that gives them full visibility into the system, so these forensic guys don't have to set foot on the client's premises. They didn't develop the software because of COVID-19, but it's been a huge boon that they've been able to use this technology to do all the forensic investigations remotely.

Has the pandemic had any impact on the type of work that your clients have been asking you to do?

It's definitely changed. A lot of companies are really suffering and looking for any opportunities to save money. So any projects that were kind of nice to have, like we should really rethink the way we're doing a vendor management program or the way in which we collect information, a lot of that stuff has slowed down, because companies don't want to spend the money and they don't have the time.

Obviously the strict compliance stuff, like complying with the California Consumer Privacy Act [which took effect in January], that's continuing. And then a huge amount of time people are spending, particularly the large multinationals, on all the privacy and data security stuff that's associated with returning to work. I don't know what percentage of my practice now is COVID-related, but it's a ton. We've been tracking all of the guidance from data protection authorities around the world and have links to all of them on our website, because so many of our clients are coming to us and saying, "We have employees in Spain, Japan, Brazil and Kansas. What can we do [when it comes to data collection]."

And we have so many clients that are getting hit by various types of malware and ransomware, so we're spending a lot of time on that as well. We had one client where they got [locked out of their system] and law enforcement said, even if you pay, you wouldn't get the key back. The company thought it would take them about 10 days to reconstitute their system, so they thought they were going to have to furlough all of their employees for 10 days. It's terrible, because the company's fighting for survival because of COVID, and now they have to lay off all of their people for 10 days. So the seriousness of these attacks, the pain that's being inflicted, is just worse than what we've seen in the past.

How has the pandemic affected companies' efforts to comply with global privacy and data security rules as well as long-standing efforts to get more laws of this kind on the books at both the state and federal levels?

The U.K. data protection regulator has talked about the fact that they may actually lower the fine that they had said they intend to impose on British Airways, because when they calculated that fine based on their revenue, it was pre-COVID, and British Airways is in a very different position now than when that intent to fine by the U.K. was issued. But it remains to be seen how much other regulators, like the Federal Trade Commission and state attorneys general, are going to take into account the extraordinary circumstances we're in right now and whether they'll be a little more empathic [when it

comes to these sophisticated nation-state cyberattacks] to the fact that the companies are the victim.

Also, pre-COVID, there were a gazillion bills that were pending in a bunch of the state legislatures, and those have all just gone dark. At the federal level, maybe we'll end up with a bill that's specific to contact tracing, but for all of the reasons that privacy legislation hasn't happened in the last 10 years, I just don't think this is the moment where there's going to be bipartisan agreement on anything with respect to personal information.

With no apparent end to the public health crisis in sight, is MoFo planning to conduct another survey in the future, and where do you expect privacy and cybersecurity concerns to rank among GCs then?

We don't have anything set, but I would think that we would do another survey. I think the privacy numbers are going to come down and a good balance between privacy and the well-being of employees will be found. A lot of people view privacy and security as being polar opposites, but I'm hoping that one of the things that happens as a result of this situation is that it shows that they can work hand and glove, and that we don't have to give up all of our privacy in order to make sure that COVID isn't spreading.

But the cybersecurity stuff, that's going to continue. There are more breaches and they're more serious, and as more companies get hit and as more companies give notice, I think that's going to continue to be a real struggle.

--Editing by Aaron Pelc.