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

7 Questions For Covington EU Privacy Chief Daniel Cooper

By **Richard Crump**

Daniel Cooper

Law360, London (March 5, 2021, 10:06 PM GMT) -- Daniel Cooper joined Covington & Burling LLP in 1996 as an associate in Washington, D.C. before moving to London two years later, at a time when data privacy was still in its infancy. His career, Cooper says, "demonstrates that life is all about timing."

"At the time it was a very unpopular subject. It was considered a bit too cerebral, arcane or off the beaten track," Cooper said. "It wasn't as sexy as frankly it is now."

But that meant he could advance in a field that wasn't saturated with other lawyers.

"You didn't have to be 80 years old and have a head of white hair to be seen as having credibility, and so I was able to learn from the very beginning when the field took off," he said.

Here, Cooper, who was appointed to lead Covington & Burling's European data protection practice in September, talks to Law360 about how data privacy practice has developed over his career and discusses the latest trends in litigation and enforcement.

How did you end up specializing in information technology regulation and data security?

An opportunity came up to go to our London office, and that was 1998. To be quite frank, there wasn't a lot of privacy work going on at the time.

I remember going to conferences to speak and it was almost like everyone was embarrassed to be there. You were in this group of people who were focused on this really obscure topic and you hoped it didn't get out to the wider public because it was just so odd. Obviously, I am saying that a little bit flippantly, but it wasn't a very popular subject.

But 1998 was a pretty important year. It was the year member states were due to implement the EU Data Protection Directive, so at the time we saw a rush of countries implementing their laws, including in the U.K. with the Data Protection Act 1998.

We started to get questions from clients about privacy issues, and really kind of baffled and befuddled by this new regulation on personal information. It was really the first time the rubber hit the road for a lot of our clients.

How have data privacy practices changed since then?

It has become more globalized through the proliferation of data protection laws. It's no longer advising on the U.K. data protection statute. Clients generally want you to advise regionally or globally.

Because of the march of technology, the growth of the internet, online platforms, social networks, artificial intelligence, blockchain, things like that have thrown up so many very complex, very challenging legal issues.

We are now at this stage where we have got these principles, and applying them in these technological contexts is very tough. This is what everyone is struggling with. What's the sensible application of general privacy norms in areas where you have to grapple with how the technology works?

What skills do lawyers need to succeed in a data privacy practice?

You have to have great analytical skills to do well in this field. A lot of the work I do deals with companies releasing products, so you have to be able to really analyze those products and understand how they work and apply these rules.

A good counsel has a keen awareness of the risks, and that is based on a really firm understanding of the law and an intuition of where the law is going to go.

That could be launching a product, changing how a service works, engaging in a certain transaction, collecting information in a certain way. Those all come with risks these days.

How will Brexit affect U.K. data privacy law?

For the next four to six months being in the U.K. from a data protection point of view will be very similar to being in the EU. But, after that, the English courts will make up their own minds about how to apply GDPR principles, and they may come to different conclusions than the EU courts.

Inevitably, there are going to be fissures opening up between the two regimes, notwithstanding the fact that English courts will take on board what the EU courts are saying and vice versa.

From a U.K. point of view, there is going to be a desire to facilitate trade with third countries. That will include trade in data, so there is going to be strong incentives for the U.K. to adopt more flexible approaches than the EU.

How the U.K. approaches things like what constitutes personal data may take a slightly less formalistic approach than the EU, [which] has narrowed the concept. How the rights of individuals are applied — that may also change too.

What developments are you seeing in data protection litigation?

We are seeing many more cases where individual claimants are bringing causes of action based on alleged privacy violations, and particularly in the U.K. courts, where you have individuals either individually or more frequently now as a class bringing claims. We had not seen that previously.

Mostly companies were more concerned about regulatory enforcement, but we are seeing a paradigm shift now as we move into a time when privacy claims are becoming a bigger threat to organizations.

U.K. courts seem supportive of this in some respects, with some of the rulings developing an independent tort related to misuse of personal information on top of claims brought for statutory violations of statutory duty in GDPR.

We are going to see more of this in the future that is spurred by these legal developments and a more aggressive plaintiffs' bar looking to enroll potential claimants.

When I advise clients, perhaps formerly it was a question of advising them on regulatory proceedings and risks of those arising. It is now more equally about the prospect of complaints and civil causes of action being launched.

What enforcement trends are you seeing in data transfers?

We are seeing more enforcement as the cases that have been pending for a while now under GDPR are getting to the end of their pipelines. It takes a while for those cases to be investigated, considered and then result in a potential fine or an actual fine.

We are seeing a lot more cases being spurred by privacy activists who are launching complaints, and regulators can't ignore these. Under GDPR you can bring a claim against a regulator for being derelict in their duty, so they can't just ignore it.

In the world of enforcement, there are a couple of knotty problems that really need to be solved.

One is how to get consistency in the level of fines being applied to companies so that similarly situated companies are handled in the same way, no matter where the regulatory action is brought.

The second is who should be responsible for bringing these investigations and imposing these fines, because right now there does seem to be a lack of coordination among regulators.

There is a lot of hand-wringing over what is the appropriate level of fines to be applied to these companies. The EU is still fractured in the way that regulators determine fines, and it is still fractured as well in who takes responsibility for bringing these cases.

The one-stop-shop principle has been a contentious topic where a number of EU regulators have felt they have jurisdiction over cases where the relevant defendant may be mainly established somewhere else.

How has the pandemic affected data protection?

Among the different states there seems to be no kind of consistent approach or attitude toward the best way to manage the privacy risks.

Certain countries have passed regulations in response to COVID-19 that require certain information to be collected by organizations about their employees and their customers. So they are putting that on a statutory footing, whereas in other countries the regulator has gone out of its way to say employers shouldn't be asking for this information, that there are privacy rights involved.

This came up in connection with some of the advice we are giving clients who may have establishments in different countries and who are trying to get a single approach. The laws and approach seem to be very different, even though everyone is suffering from the same issues, the same phenomenon.

It will be very interesting in the years ahead to see if COVID-19 has changed how employers and employees view privacy in the employment setting.

Everyone appreciates this is a pandemic...however, will that reset expectations and how employees view their privacy vis-à-vis their employers? Will that result in a relaxing of attitudes or will we swing the other way, and will employees become more obsessive and protective of their privacy?

--Editing by Joe Millis.