Corporate Counsel Business Journal

May • June 2020
CCBJournal.com

CCBJ

Antitrust Regulation in the Era of Big Data and COVID-19

▶ Andrea Levine, managing director with FTI Consulting, discusses various aspects of antitrust enforcement in 2020, from data collection in a cloud-based world to how companies are coping with the effects of the pandemic.

CCBJ: Tell us about your experience prior to joining FTI.

Andrea Levine: I was an attorney at Simpson Thacher & Bartlett in New York City. I specialized in various antitrust matters, specifically merger enforcement and some cartel work. In merger reviews, if the FTC or DOJ undertakes a more fruitful investigation, they'll issue what's called a Second Request, asking for a large volume of information related to the merging parties and their industry. These cases – and my work on them – have always been at the forefront of e-discovery. These matters are both very data intensive and operate on a very quick timeline. So that's how I came to know FTI: We would often engage them to help us comply with these requests, quickly and comprehensively.

COVID-19 has disrupted how companies and employees work. What do you think its downstream impact on investigations will be?

From my perspective, one of the biggest impacts of COVID-19 on businesses is the shift to a largely remote workforce. Approximately 60 percent of employees right now are working from home, and from a data and investigation perspective what we're seeing is that a lot of these employees are looking to use various kinds of software, particularly collaboration and video software like Microsoft Teams or Zoom, to stay in touch with colleagues and clients and continue to share information – verbally, of course, but they're also creating shared repositories for documents and data. And depending on a company's mobile device policy, we're seeing a lot more employees using personal devices like smartphones or tablets to conduct business. So data is being created through a variety of sources and at a greater extent than before. And because this was a pretty quick shift and companies weren't planning to shift their workforce to home, there are a couple of things they may not have been prepared for. One, they don't necessarily know all of the different applications that their employees are using because solutions are being created on an ad hoc basis, and two, how to preserve, collect and process all of that new information that's being created. Specifically looking toward investigations, if the time comes that they have an internal complaint or there are government requests for information, the first step they'll have to take is identifying all of the various ways in which data was created, and how all of that information is being stored, and then only then can they think about how to collect, review and produce that data.

Another aspect to consider is that when we think of data collection, currently – or in the very recent past – a lot of it is being done by IT departments themselves. A lot of that data, especially if it's organized and maintained properly, can be pulled on the back end by IT, and that saves time and money in an investigation. But now, as people are creating data in new applications, and saving data locally on their computer or mobile devices, IT staff does not have access to this data and companies will need to perform remote data collections if an investigation arises before employees can return to work. Relying on the employees themselves to properly collect all of the potentially relevant data creates additional complexities, because if you're obligated to produce this data for a government investigation, or a litigation, you need to ensure that your collection is comprehensive and defensible. That's not typically part of an employee's day-to-day responsibilities, so you have to ensure knowledgeable people are overseeing collections and making data is being collected in the right way.

These changes in data creation and preservation also implicate privacy issues, and at least in the case of cartel

investigations, across several jurisdictions with varying regulations. In the last several years, we've seen an increase in privacy regulations, most notably the General Data Protection Regulation (GDPR). To the extent that you are creating, collecting, or storing data globally, and potentially moving it across borders, you'll potentially trigger these various regulations. You want to make sure that everything you're doing around these emerging data sources does not run afoul of those regulations. As a company, at the forefront of your mind is not only knowing where your data is and how you can preserve and collect it but also how you're protecting it and transferring it as needed.

What do you think the priorities and expectations will be from antitrust regulators conducting investigations?

We can expect that the agencies to request data from emerging data sources, particularly those that facilitate communications across companies as the DOJ is required to provide evidence of an illicit agreement in cartel cases. We started to see that even before COVID-19 – people were shifting to working from home even before that – and the regulatory agencies, particularly the DOJ, demonstrated an interest in different data types. For example, last November, a former JP Morgan trader was convicted of conspiracy in a scheme to rig the global foreign currency exchange. And the basis of that conviction was in part drawn from text messages and online chat rooms. So that's been a really big focus for the DOJ. We had already started to see that shift away from the typical email documents and into these other kinds of online communications.

As a company that works in this space, we've seen the same trend, of course. In the last two years, we've produced data from cloud-based collaboration software and mobile messaging apps in response to Second Requests.

In addition to prior cases, we've also seen the DOJ update their guidance to specifically address data issues and new data sources. One example is the DOJ Antitrust Primer for Federal Law Enforcement Personnel. Their internal guidance was updated in September 2018, and now it specifically mentions that evidence of illicit communication and cooperation among competitors could take the form of, and these are their words, "emails, text message, Facebook messages, WhatsApp and encrypted messaging apps." So they're publicly articulating how broad their definition of relevant data is, as well as where they're specifically looking to find evidence of these conspiracies.

This year, we've also seen revisions to the DOJ's guidance on corporate compliance policies. The latest revision adds that in determining the effectiveness of a company's anti-

> As data storage shifts to the cloud, cybersecurity threats become more real than they were before.
>
> — ANDREA LEVINE

trust compliance program, the DOJ will consider whether "compliance and control personnel have sufficient direct or indirect access to relevant sources of data" and whether any "impediments exist that limit access to relevant sources of data." In order to determine whether a company is being proactive in rooting out misconduct, they want to see that the personnel running the audits are able to view all of the relevant data, and do so on a periodic basis, not just one snapshot in time. This suggests that difficulty around collecting from disparate data sources does not excuse companies from monitoring this data, let alone excuse companies from providing them in response to government inquiries.

One other thing I wanted to add is that while we are in the midst of a pandemic and an economic shutdown, these factors can actually trigger potential misconduct in the antitrust space. The reason being that there are some companies that are typically competitors but are now working together in joint ventures or other arrangements to address the pandemic. Naturally we think of that as pro-competitive, but it also opens doors for behind-the-scenes communications between competitors, and the possibility that they inadvertently or intentionally share competitively sensitive information. That's something that regulators may be on the lookout as more of these joint ventures arise.

The other aspect of this is that coming out of this economic shutdown, companies may feel pressure to make up for the revenue that's been lost. Those pressures can create situations that are ripe for potential misconduct. So I think it's important for companies to start taking their antitrust risks seriously right now, especially if they are part of a joint venture, or if their field employees are under pressure to make up for lost sales, lost business. Start thinking now about how you're going to get in front of any misconduct, how you're going to find it if there is any, and again, how to put compliance programs in place to make sure that you can do it effectively.

How can in-house legal teams prepare themselves?

The best thing they can do is make sure their companies get in front of these issues by implementing a comprehensive information governance policy. That goes beyond just having a policy on paper where you tell employees what records to preserve. You have to also take a look at all of the various sources of data, how that data communicates with each other, how it travels through the company. Through that process, you can identify where the data is being created, where it is being stored, how easy it would be to preserve or collect, and whether it can be consolidated into central data systems. And, of course, how to access it for investigatory and litigation needs. Certain applications don't work seamlessly with existing data collection and processing software so it's important to think ahead to how you would address those issues.

Another aspect of information governance is how the data is organized. In information governance, we think about what data a company is legally required to store, what it makes sense to delete, what it needs to protect. But we also think about how data is organized by department, by project, by type of communication. This type of structure allows for more targeted data collection which saves time and costs associated with processing, hosting and reviewing data. Conversely, if the data is all mingled, you need to pull from all potentially relevant data sources significantly increasing the initial data volume.

Let's talk about what role service providers can play in preparation and response.

Service providers have a level of expertise that companies themselves are not likely to have. They not only understand the complexities around new data sources but are also experts in how to tackle them to meet a particular company's needs. There are considerations around retention needs versus the cost of storage, as well as balancing the need for data security with ease of collection. Service providers can walk a company through its options and recommend the policies and software that will work best. And as data storage migrates to the cloud, cybersecurity threats become a greater concern. It's not only a matter of knowing where your data is and complying with preservation regulations but also ensuring that your company's data does not get hacked or even misappropriated within the company. A service provider can determine where the security risks are by looking at your current data management system, where the risks are and present solutions to increase data security.

What other considerations should legal teams be thinking of as they continue to adapt to the current environment?

COVID-19 has significantly changed the way employees do business and many of these changes, working remotely, communicating on mobile devices, not being connected to a company network, sharing documents and messaging through cloud-based software, impede a company's ability to readily track and access data in a systematic way. Moreover, these newer apps are seeing significant increases in use and their systems have not necessarily been tested, from a security perspective, in this way. I'm thinking of Zoom in particular, that has become the video conferencing software of choice for many organizations now conducting business virtually. That app has just exploded since the shelter in place orders started. This security concern is one of the best arguments, aside e-discovery needs, for having an information governance policy in place: There is just so much personal data out there, personally identifiable data, personal health information, credit card information, Social Security numbers and the like. If a company is not proactive about protecting that information, it's potentially out there for the taking. And when I say protect, I'm anticipating that companies have done some level of work to protect their data, but as the location of this data changes, companies need to adapt to the new risks and put security additional measures in place.

> Coming out of the economic shutdown, companies may feel pressure to make up for lost revenue, which can create situations that are ripe for misconduct.
>
> — ANDREA LEVINE

In short, this major transformation in the workplace can create a number of headaches for in-house legal down the road, from lengthy and complicated document collections to data security breaches. But with foresight and the right expertise, they can identify the issues now and avoid costly and time-consuming problems later. ■

Andrea Levine, is a managing director within the technology practice of FTI Consulting and is based in New York. Ms. Levine advises clients on the use of advanced analytics technology and methodologies to expedite fact-finding and case development for investigations and complex discovery matters. Reach her at andrea.levine@fticonsulting.com.