Interview with Maneesha Mithal, Associate Director, Division of Privacy and Identity Protection, Federal Trade Commission

Editor's Note: Maneesha Mithal has served as the FTC's Associate Director for the Division of Privacy and Identity Protection for 10 years. Ten years prior to that, she moved from private practice to the FTC, where she held a number of positions before becoming Associate Director. During her time as Associate Director, Maneesha has had a front row seat as privacy law and privacy concerns have rocketed to the forefront of all our consciousness as we have all become familiar with privacy acronyms such as GDPR in the EU and California’s CCPA. She has also presided over a period of active FTC education, guidance, and enforcement in the consumer privacy space, playing an important role in last summer’s $5 billion settlement with Facebook over allegations that it had violated a prior consent order governing how it should handle consumers’ personal information.

The interview was conducted for The Antitrust Source by Randal Shaheen, a partner in the Digital Assets and Data Management Practice Group at BakerHostetler LLP, and an Editor of The Source.

ANTITRUST SOURCE: Thank you Maneesha, I know that there's a lot going on in the privacy world so I appreciate you taking the time to speak with me.

MANEESHA MITHAL: My pleasure.

ANTITRUST SOURCE: Before we delve into substance, could you just talk a little bit about your background and your time at the FTC?

MANEESHA MITHAL: Sure. I have been at the FTC for about 20 years. Prior to that, I was in private practice in the litigation group of a big firm. During my time at the FTC I've had many roles. I started off in the International Consumer Protection Division, then I was Chief of Staff for Bureau Director Lydia Parnes. From there I came to DPIP (Division of Privacy and Data Protection) to work on privacy issues, first as a staff attorney and now as the Associate Director. I've held this last position for about 10 years.

And I would say that every job I've had prior to this has prepared me for being in the privacy space. When I graduated from law school, privacy wasn't a field or a profession for lawyers. But I had a litigation job and then I had an international job where I did a lot of privacy work and saw how Europeans view privacy. I worked in the FTC's international division right after the EU/U.S. Privacy Safe Harbor was negotiated.

And then when I was Chief of Staff for the Bureau Director, I got to interact with the Commissioners on a host of issues including privacy. Finally, as a staff attorney in DPIP, I got to work on privacy cases, as well as a privacy rulemaking—the Health Breach Notification Rule. And so over the course of several years, I developed an interest in privacy. Each of the positions I had held prepared me to become Associate Director of DPIP in 2009.
**ANTITRUST SOURCE**: I imagine being in this job for 10 years is like a lifetime in terms of developments in the privacy space.

**MANEESHA MITHAL**: Absolutely, and I think one of the things that’s really interesting is that when I talk to people who just graduated from law school, what an interest there is in the profession and how much growth there is in the profession. For example, when I started going to the meetings of the International Association of Privacy Professionals, it was a couple of hundred people and now it’s several tens of thousands of people in that group, so the profession has grown by leaps and bounds.

**ANTITRUST SOURCE**: There are, as you know, a lot of different divisions at the FTC with different responsibilities. Do you find yourself interacting pretty frequently with the other divisions at the FTC?

**MANEESHA MITHAL**: Yes, we interact with a number of the other divisions in the consumer protection area. For example, the heads of each of the divisions meet every week, and we identify issues where there’s overlap or cases where there may be overlap.

And we’ve worked with other divisions on many matters. The most recent and pretty noteworthy example is the Facebook matter. Our division negotiated the original consent order from 2011 and then, most recently, when there were allegations of non-compliance, the enforcement division got involved as they act to enforce all of our consent orders.

The enforcement division had the lead on the 2019 Facebook settlement, but we worked very much hand in hand with them. Attorneys from both divisions were staffed on the case.

There are also financial privacy issues that come up. For example, the Division of Financial Practices is litigating a case against Lending Club, and there’s a Gramm-Leach-Bliley privacy count in that case, alleging that the company failed to provide a clear and conspicuous privacy notice. Finally, we see cases that have privacy components and deceptive advertising components, and we work together with other divisions on those.

**ANTITRUST SOURCE**: It does seem like the privacy and consumer protection worlds are intersecting more and more.

**MANEESHA MITHAL**: Yes, absolutely, and when you think about privacy law at the FTC, most of it is based on Section 5’s prohibition of unfair or deceptive practices. Our work builds on the work that the Division of Advertising Practices has done on deception and the elements required to establish it.

**ANTITRUST SOURCE**: I want to talk about enforcement in a second, but on the education side, one thing I hear people say is that while they have all these privacy rights, they don’t really know what they are and how to trigger them. Is the FTC engaged in trying to educate consumers with respect to what privacy rights they have and how to assert them?

**MANEESHA MITHAL**: Yes, the FTC has done a lot of work to educate consumers. The most prominent example is our IdentityTheft.gov website where consumers can go if they’ve been a victim of a data breach or if they have been a victim of identity theft. That website is a one-stop shop where consumers can go to learn about these issues and figure out what steps to take.
On privacy more generally, we have a number of materials on our website. We have, for example, videos on how companies use your data. We have more specific items on things such as cookies and how you can opt out of certain tracking online.

But perhaps the most significant way we get our message out to consumers is that every time we have an enforcement action where we think there is an important lesson for consumers, we put out information on our consumer blog. One recent example is a case we brought against a company that manufactured a stalking app, spyware that secretly monitors smartphones. We then worked with the domestic violence community and put out consumer messages on how you could tell if there’s a stalking app on your phone.

We use our cases as a vehicle to talk to consumers. Our award-winning Division of Consumer Business Education also has a lot of modules where they train the trainer. They’ll go out to senior centers or libraries and they’ll put our publications there and then hopefully that has a ripple effect where community leaders can tell people about privacy and other issues affecting consumers.

**ANTITRUST SOURCE:** Many people have noted that the FTC is in somewhat of a unique situation in terms of having five brand new commissioners, though I guess increasingly they’re not so new anymore. How engaged have you found them on privacy issues?

**MANEESHA MITHAL:** All five of them are incredibly engaged, and I think you saw that from some of the big cases we announced last year. They were very heavily involved, and I think they asked a lot of terrific questions.

It’s nice for us as staff who have been here for a long time to have bosses who are really engaged in our work and want to advocate for it. While we knew that Chairman Simons has an extensive antitrust background, we were wondering what his level of engagement would be on privacy. And he has turned out to be incredibly engaged. He has been supportive of all of our big cases, and he came right out of the gate with the hearings on competition and consumer protection, wanting us to look at how we can have better remedies in privacy and data security cases. He has supported congressional legislation on privacy and data security issues.

**ANTITRUST SOURCE:** Turning to enforcement, we read about data breaches all the time. It seems like almost every day someone has a data breach somewhere. I believe it was Chairman Maureen Ohlhausen who noted that the FTC doesn’t open an investigation every time there’s a data breach. What factors go into deciding if you’re going to investigate a particular data breach?

**MANEESHA MITHAL:** There are a number of factors that go into it. First is the size of the breach. Obviously a larger breach is going to get our attention more than a smaller breach.

Second is the sensitivity of the data. We’d be very interested in a case where we thought that a company might not have protected Social Security numbers, for example, as opposed to a list of names or public information.

A third factor is likelihood of harm. For example, let’s say we hear about a vulnerability in a particular product, but the path to exploiting that vulnerability would require several steps and it would be unlikely for that vulnerability to be exploited. I think we would be less likely to bring that case. Or, suppose there is data that was breached but it was encrypted. I think in that situation, we would probably be less likely to open an investigation unless, of course, the encryption key was included with the data breach.

**ANTITRUST SOURCE:** There’s also been a lot of discussion in the consumer protection space...
about remedies, and it’s one of the areas that Chairman Simons and the other commissioners have said that the Commission should take a fresh look at. On the privacy side specifically there has been some debate about when monetary remedies are or should be available.

What are the range of remedies that are available and how do you settle on a particular remedy in a particular case?

**MANEESHA MITHAL:** If you look at some of our prior orders, you’ll see we have a range of remedies. In deception cases, our settlements typically prohibit specific misrepresentations regarding privacy.

Sometimes, we have provisions requiring deletion of data and notices to individuals. In a case from last year, a company called Unroll.Me operated a service that helped you manage your inboxes. There were some consumers who declined to participate. The company tried to reassure consumers who declined to participate because of privacy concerns and said, “Don’t worry, we won’t touch your personal stuff.” But in fact, we alleged that they took consumers’ e-receipts and shared them with another company that, in turn, used that information for marketing. We alleged that was deceptive.

In addition to a “do not misrepresent” provision, the order included a requirement that the company delete the data that it had collected. It also included a requirement that the company provide notice to consumers about how it used and shared consumers’ information.

We have also sometimes required companies to undergo comprehensive privacy assessments. Facebook and Equifax are notable examples of where we required companies to engage in a comprehensive risk assessment on either privacy or security and to get their programs audited by an independent third party.

Those are some of the types of remedies we look at on the injunctive side. And of course, where we have civil penalty authority, we would look to impose civil penalties on the company in appropriate cases, depending on several factors.

**ANTITRUST SOURCE:** The Commission ran into a bit of a hiccup in court on some of its injunctive relief language, which caused the Commission to introduce some new language. Has that roll out gone pretty smoothly?

**MANEESHA MITHAL:** Yes. There were a couple of things that happened last year that made us take another look at some of our orders. First is the case you are referring to which is the Eleventh Circuit decision in LabMD, where we had required the company to have a reasonable data security program and the Eleventh Circuit said that requirement wasn’t specific enough.

The second thing that happened last year, as you alluded to, is that Chairman Simons asked us to relook at some of our orders and some of our remedies. Based on that feedback, we’ve announced orders in seven data security cases last year, and if you look at them, I think we have made improvements in three areas.

The first is we’ve made the orders more specific, so in addition to requiring a comprehensive data security program, we have required things like encryption and access controls and training, in part to respond to the Eleventh Circuit. The second thing is we have tried to improve the accountability of third-party assessors. Our prior orders required companies to get outside assessors biannually. We’ve now added a provision that gives the FTC the right to approve the assessor for each two-year period. So, if we are not happy with the job the assessor has been doing, then we can tell the company that they have to pick a different assessor.
The third thing we’ve tried to do is to elevate security and privacy issues to the board level. If you look at some of our new requirements, we talk about having a written program that’s reviewed by the board. And we also talk about requiring individual certification by an officer or a senior person at the company. One of the statistics we’ve seen is that companies are 35 percent less likely to be breached if they have a CISO, a Chief Information Security Officer, who reports to the board. And so that is something that we’re trying to include in our orders.

ANTITRUST SOURCE: I’ve been watching this debate with interest because I can remember a time when, with respect to advertising orders, some companies were complaining that the requirement for competent reliable scientific evidence to support certain product claims was too vague. Then the Commission rolled out a new, more specific definition for the term and then many companies began to complain about the lack of flexibility.

MANEESHA MITHAL: Yes, exactly, right. Well, we’re seeing the same debate play out in our Gramm-Leach-Bliley (GLB) Safeguards Rulemaking. The GLB Safeguards Rule was passed in the early 2000s and imposes data security requirements on financial institutions. After it passed, companies said, “Oh, this is not specific enough, we need more guidance.” We’ve responded with a notice of proposed rulemaking where we have tried to fill in some more meat on the bones of the GLB Safeguards Rule. In the initial round of comments, we got some supportive comments, but we got some companies saying, “Oh, this is too specific.” We are reviewing these comments and trying to develop a final rule with the right level of specificity.

ANTITRUST SOURCE: I’m wondering if you have advice for a company that has a data breach and then they get a CID from the FTC. Obviously they need to begin preserving relevant documents, but is there any other advice you would give in terms of engaging successfully with your staff that companies should think about doing sooner rather than later?

MANEESHA MITHAL: Yes, I’d offer a couple of pieces of advice. First is that oftentimes when companies get CIDs, they try in their responses to hew very specifically to the questions that we ask. I would tell a company if you have a story to tell, tell it even if we haven’t asked the specific question. Because a lot of times if a company comes in and tells an affirmative story about the lack of likelihood of harm or the specific pieces of data that were breached and all of their mitigation efforts, in some cases we might elect to close the case early on, rather than having the company spend a lot of money to respond to the CID. I think telling your story and telling it early is really important.

The second thing is that a lot of companies make overbroad assertions of burden. Your objections are much more likely to be successful if you can pinpoint where the problems are and give examples, not just make a broad proclamation of burden. The more specific examples you can provide, the more helpful it is to us.

The third thing I would say is to work with the staff. I think some counsel, particularly repeat counsel, have a tendency to want to escalate up the chain early and I think that’s very counterproductive. The best outcome is to get the staff on your side because they’re the ones who are going to advocate to people at more senior levels. And so I think trying to work with staff and then, only if you don’t get the result you want, going up the chain is the best approach.

ANTITRUST SOURCE: OK, don’t jump the line.
MANEESHA MITHAL: Yes, nobody wants a line jumper. Having said that, we don’t punish companies because their counsel does things we don’t like. But I think that there are things you can do to help the process.

ANTITRUST SOURCE: A lot of your work involves tech companies. There has been some discussion about tech company mergers and whether privacy should be a relevant consideration in any antitrust review of proposed mergers. For example, will a merger stifle competition with respect to privacy policies. Do you weigh in sometimes on those issues?

MANEESHA MITHAL: Yes, we work really closely with our counterparts in the Bureau of Competition, particularly the technology enforcement division. We meet regularly. We try to identify issues and areas of interest to both competition lawyers and privacy lawyers. And while I’m not an antitrust lawyer by any means, one thing I understand from my antitrust colleagues is that they do consider aspects of privacy competition in mergers. I expect going forward, we will be working with them very closely on this question.

There are also other examples in the past where we have worked closely with our Bureau of Competition counterparts. An example that comes to mind is the Facebook/WhatsApp merger, where our antitrust colleagues looked at it and the FTC staff sent a public letter to the company reminding them that their respective consumer protection statements continue to apply even after the merger. In general, I think we are seeing more and more interest in the intersection between competition and privacy and it’s something that we are looking at closely.

ANTITRUST SOURCE: January 1, 2020, is the CCPA (California Consumer Privacy Act) roll out in California. I’ve read that the California AG’s office has been staffing up in anticipation of numerous enforcement actions. Do you foresee a role for the FTC with respect to CCPA or is this really more of a state issue?

MANEESHA MITHAL: I don’t see a specific role for the FTC in enforcing the CCPA. That will be up to California state authorities.

ANTITRUST SOURCE: Suppose a company goes further and says, “We’re going to be CCPA compliant not just in California, but nationwide,” and it turns out that in Iowa or Nebraska allegedly they’re not. That doesn’t seem like a promise California can enforce. Is that a claim that the FTC would potentially enforce?

MANEESHA MITHAL: I can’t think of any case where we have done something like that. On the one hand a claim like that could be deceptive. On the other hand, we’d have to determine whether the company was in fact compliant with CCPA in those other states, and it’s difficult to ask us to opine on the parameters of state law and what it does and does not require. I think that’s something we’d have to look at on a case-by-case basis.

ANTITRUST SOURCE: Whether they’re actually compliant with CCPA in other states?

MANEESHA MITHAL: Among other things. But I think this shows one of the things that people talked about at the Congressional hearing this morning—that privacy doesn’t stop at state lines. For example, you’re engaged in a transaction, using a phone with an area code from a place you used
to live in, and you’re sitting in Washington D.C., ordering from a Californian company and shipping the goods to your sister in Ohio. Which state’s privacy laws apply? I think this illustrates the need for federal legislation in the privacy area.

ANTITRUST SOURCE: That’s a good segue for my next question, which is about the hearing today and the federal legislation that’s being considered. Has the FTC taken an official position on a federal privacy bill or federal privacy legislation?

MANEESHA MITHAL: Yes. The FTC supports a comprehensive federal privacy law. The law we’ve recommended would have four key components. The first is the ability to fine companies for first-time violations. Right now, we have to wait to get a company under order and then we can obtain civil penalties for any violation of that order.

Second is targeted APA (Administrative Procedures Act) rulemaking authority so that we modify regulations and requirements as technology evolves. Third is jurisdiction over common carriers and non-profits. Last is additional resources for the FTC to enforce a new privacy law.

One model that people have talked about as a potentially good model for how to include these types of provisions is COPPA (Children's Online Privacy Protection Act). The FTC has civil penalty authority under COPPA. In terms of APA rulemaking authority and the ability to adapt to new technology, when Congress enacted COPPA in the late 1990s, kids weren’t uploading their photos onto social media. Kids also weren’t carrying around their geo-location information in their pocket. And so we were able to update COPPA in 2013 to take into account these changes in technology, and I think that would be really important in any federal privacy law.

ANTITRUST SOURCE: Let me ask you about data exporting. The EU has restrictions on data exports on the theory that you shouldn’t be able to take consumer data out of a country and then it loses whatever protections it originally had. Has the FTC given any thought to whether there should be restrictions like that in any federal privacy law?

MANEESHA MITHAL: Yes. The EU has certain restrictions on cross-border data transfers unless the recipient country has adequate protection. I think what we’ve always said in the U.S. is that we really need to balance people’s legitimate interest in protecting the privacy of their data with the need for the cross-border free-flow of data.

We would leave whether to include such protection and how to specifically balance those competing interests to Congress, but I think that to the extent that any requirement is considered along those lines, we’d want to balance the cross-border flow of information with privacy interests.

ANTITRUST SOURCE: I’d like to conclude with a couple of general questions. First, are there particular areas of privacy or data security that the FTC is particularly concerned about right now?

MANEESHA MITHAL: Sure. An evergreen concern is the misuse of sensitive information. Within that broad category there are a couple of areas we’ve been focused on. The first is health information. We’ve brought a number of cases in the health area, particularly with respect to companies like data brokers and health apps that are consumer facing that are not necessarily covered by HIPAA (Health Insurance Portability and Accountability Act), yet they collect very sensitive data. And so that continues to be an area of interest for us—non-HIPAA covered entities that are collecting health information.
I think another area is monitoring the content of communications. An example of this is the Retina-X case, which is a stalkerware case where the company permitted surreptitious monitoring of the content on someone else’s device.

Kids’ privacy is also always a front-and-center issue for us. On the technology front we continue to be interested both in privacy and data security involving the internet of things, e.g., connected devices. We just settled our D-Link litigation earlier this year, where we alleged there were security vulnerabilities in the company’s routers and internet-connected cameras.

In terms of emerging areas—artificial intelligence, machine learning, algorithmic biases—these are issues that we’ve been working on for the last couple of years. I think you’re going to be hearing more and more about privacy and data security concerns related to these areas. And we had a hearing on artificial intelligence last year.

**ANTITRUST SOURCE:** How do you and your staff keep abreast of all these developments. It changes so fast, and it can be so complex. I assume you must have non-lawyers who assist you?

**MANEESHA MITHAL:** Yes, I think it’s really important to stay on top of the technology, and we do that in several ways. We have our Office of Technology Research and Investigations which often helps us generate case leads. This office does original research. For example, they did a recent study where they posted consumer data sets on a site frequented by identity thieves, and they saw that the first use of the data occurred within nine minutes of posting.

A second way in which we get information is through an annual conference called PrivacyCon. As part of that conference we solicit original research on various privacy and data security issues, primarily what are the new issues, what are the things that technologists and academics are concerned about in the privacy area? We get numerous papers, and we review those papers and we generate case leads through that.

We also try to be smart in our hiring. We’ve hired people who have tech backgrounds, who are interested in technology, who have a lot of capacity for looking at technology issues.

The final thing I would say is that we often supplement our in-house expertise with technology experts. In many of our data security cases, we retain consulting experts on data security as the needs arise.

**ANTITRUST SOURCE:** One last question. *The Antitrust Source* spans both consumer protection/privacy and antitrust. For those of our readers who may be very familiar with antitrust law but not so much with consumer protection or privacy, what are some essential things antitrust lawyers should know about privacy law?

**MANEESHA MITHAL:** I was talking to an antitrust lawyer who said that she didn’t appreciate in advising merger clients that the statements the companies made to consumers pre-merger relating to privacy and data security may continue to apply post-merger. The WhatsApp letter that we did a couple of years ago where we reminded Facebook and WhatsApp of their obligations in light of Facebook’s proposed acquisition of the company highlights that. So as you’re advising clients on mergers, make sure that they’re continuing to comply with their commitments to protect data post-merger.

More generally, as antitrust lawyers begin to think about privacy issues, there are a number of privacy laws that practitioners might want to be familiar with. In terms of ones the FTC enforces, you have the Gramm-Leach-Bliley Act that applies to financial institutions, the Children’s Online Privacy Protection Act, the Fair Credit Reporting Act, and of course the Section 5 prohibition against unfair and deceptive practices.
against unfair and deceptive practices. I would obtain a general understanding of those laws and how they might apply to your situation.

We also have a number of tech companies under FTC orders already. Antitrust lawyers might want to look at those for clues about how we think about privacy and what we expect in terms of best practices.

**ANTITRUST SOURCE:** I imagine if you’re doing due diligence for a proposed merger, privacy and data security as well as order compliance, if one exists, have got to be important elements of that.

**MANEESHA MITHAL:** Yes, right, exactly. A lot of times when we see a big data breach occur the companies say, “Oh, this is a company that we had acquired.” But I think it’s important for the company to do that due diligence when they are considering the acquisition, so they know what they’re getting into.

**ANTITRUST SOURCE:** Thank you very much, Maneesha. I think you’ve educated us all and given us a lot to chew on.

**MANEESHA MITHAL:** Thank you, Randy. It’s my pleasure and it’s always good to talk to this audience and let them know what we’re doing.