Podcast Transcript

2024 DSIR Deeper Dive: FTC in 2024 Continues Aggressive Privacy Path – But Don’t Forget About that Rulemaking

Date: October 24, 2024

Guest: Daniel Kaufman and Jennifer Mitchell, **Host:** Amy Kattman

Run Time: 13:19

For questions and comments contact:

Daniel Kaufman

Partner
Washington. D.C.
T: +1.202.861.1523 | dkaufman@bakerlaw.com

Jennifer L. Mitchell

Partner

Los Angeles

T: +1.310.442.8865 | jlmitchell@bakerlaw.com

Kattman: On April 23rd, Baker Hostetler's Digital Assets and Data Management Practice Group released its annual Data Security and Incident Response, DSIR Report. This year marks the 10th anniversary of the report, which is now widely used by businesses all over the world to help develop their cybersecurity measures, incident response plans and information governance practices. I'm Amy Kattman, and you're listening to BakerHosts.

We're back with a Deeper Dive series covering key topics in this year's DSIR. On today's episode, we take a deeper dive into the FTC's recent privacy developments. Our guests today are Daniel Kaufman and Jennifer Mitchell. Daniel is a partner in BakerHostetler's Advertising, Marketing and Digital Media team. Prior to his current role at the firm, Daniel had a long career at the FTC's Bureau of Consumer Protection. Jennifer Mitchell is BakerHostetler's Los Angeles, San Francisco and Orange County Digital Assets and Data

Management leader and the co-leader of the Media and Telecommunications Industry team. Welcome to the show, Daniel and Jen.

Kaufman: Thank you so much. We're really glad to be here.

Mitchell: Thanks Amy.

Kattman: Jen, let's begin with you. How closely has the FTC been scrutinizing the collection of health data and why this data in particular?

Mitchell: Yeah, that is a great question. So, the FTC certainly continues to be focused on health data recently and in addition to other areas of focus like geolocation and children's data. And this is not necessarily a new trend, but it's been one that's been reinforced again in 2024. So, health data, as we know, is considered a type of sensitive data across privacy laws, and the FTC has shown special interest in scrutinizing the practices of companies that process very sensitive types of health information, such as mental health data like the Better Help enforcement action in 2023, reproductive health data like the action brought relating to the Premom app and also addiction related health information and earlier this year, the FTC announced another enforcement action against a telehealth company that allegedly engaged in the unauthorized disclosure of mental health information as well as other sensitive data to third parties for advertising purposes.

In addition to the enforcement activity earlier this year, the FTC also clarified that the Health Breach Notification Rule applies to Health and Wellness apps, meaning that these technologies will face enforcement action and potential penalties if they do not notify consumers when their health data is disclosed without their permission. So, this is important because while many digital health companies are subject to HIPAA, consumer health data that is not governed under HIPAA has not historically been subject to as robust protection. And so, as a result of these enforcement actions and the increased focus of the FTC on health data and consumer health data, we know that the key issues that companies should be thinking about is how are they collecting health information? How are they using health information? How are they providing notice, and if required, how are they obtaining consent for the use and sharing of health data? And again, in particular, the agency is very focused on whether and how that data may be used for targeted advertising.

Kattman: Daniel, what about browsing and geolocation data?

Kaufman: Thanks, Amy. So, this year and last year, we have certainly seen an increased focus from the FTC on instances where large quantities of certain sensitive data, including browsing data and geolocation data are being collected. And these have all been subject of FTC law enforcement. And again, much like Jen said, this isn't necessarily a new focus at the FTC. For example, on browsing data they've talked about that for quite some time, but we are certainly seeing more of a focus. And at the outset, identifiable or re identifiable browsing data can tell you an enormous amount about a person. And notably in one of these recent FTC cases, the data sets at issue although they removed elements such as names, Social Security number, the FTC alleged that the data was not aggregated and the company was using a separate unique identifier that made the browsing data set not anonymous because of the ability to reidentify and connect the data. And it was highly meaningful data about specific individuals. And we're seeing that also in geolocation, another really big focus area for the FTC. And certainly, the *Dobbs* decision amped up the agency's focus on both geolocation and health issues, and they really emphasized how consumers' information is being collected, what are consumers being told, and they're looking closely at whether the consumer consent there is truly informed or if, is it just buried on page seven of a privacy policy and they brought a few cases that have really beefed up the attention that companies have to take if they are collecting, sharing, using consumer geolocation.

Kattman: Danielle, will you please explain what the 2022 Advance Notice of Proposed Rulemaking is and what businesses should expect in the near future?

Kaufman: So, the Federal Trade Commission has broad rulemaking authority to issue rules involving practices that are deceptive or unfair. So, they do have this broad authority, and they started this rule making in 2022. It's been almost a full two years now, where they raised all sorts of broad privacy issues, raising from security to AI to biometrics to kids and teens data and asked literally 100 different questions. In that two years, we really haven't heard from the FTC about this rulemaking. They haven't come out with a proposed rule or anything like that. So, the short answer is companies don't need to worry about this at the outset. This is not like there is going to be a rule that pops tomorrow, that is final.

The next part of this process would be assuming it goes forward, the FTC would issue some proposed rule dealing with the many, many issues at stake. It may be about privacy policies it may be about security and it may be about teen data, it may be about algorithms. And then there'd be another lengthy process where companies would comment, and the FTC would eventually issue a final rule. But I think we're certainly, I would say at least a year or two away from any rule coming out of this rulemaking that would be close to final. And it is also worth noting that we now have a full Commission. We've got three Democrats, two Republicans, and there are going to be some very different views there on whether it is appropriate and lawful for the FTC to do this rulemaking based upon where they end up. I'm sure all five of them will be looking very closely at whatever proposal might exist, but I think there will be very different views about this rule, particularly if the FTC tries to go broad and develop some broad privacy rule akin to what the states have been doing.

Kattman: Jen has there been any movement on the children's and teens front for national privacy legislation?

Mitchell: Yes, yes there has. This is another hot topic that we've seen with FTC, both FTC enforcement as well as federal rule making and one example is earlier this year in 2024, the agency interestingly teamed up with the Los Angeles District Attorney's Office and settled against a messaging app company as well as two of its co-founders and their personal capacity relating to this messaging app and the practices of the messaging app in the sum of $5 million. And also importantly, in addition to that monetary settlement, the company was banned against offering the app to children and teens under the age of 18.

So, among many of the allegations that the complaint, which is worth reading, one focus of the FTC and the LA District Attorney's office was in relation to the use of an AI content moderation program that was supposed to filter out cyber bullying and other harmful messages to this vulnerable population and also allegations that the app caused fake messages to be sent to users of the app. And in addition to the recent enforcement activity that continues to emphasize the importance of this population in the eyes of the FTC and protecting this population, Congress continues to consider national privacy legislation to protect this population. This summer, the summer of 2024, the US Senate voted to pass the proposed bipartisan bill that combined the proposed Kids Online Safety Act or KOSA. The Children's and Teens Online Privacy Protection Act and the Filter Bubble Transparency Act. And so each piece of legislation sets out to accomplish online safety goals for different age ranges. COPPA 2.0, as it's been called, covers children under the age of 17, while KOSA applies to children under the age of 13. But both statutes would provide additional protections to kids as well as additional authority to the FTC. So, outside the subject of this particular podcast, but in addition to the FTC enforcement activity and federal rulemaking, there is, of course, substantial amount of movement in state laws regulating and protecting, further protecting children's data as well.

Kattman: Daniel, I have one final question for you. How will the Supreme Court's decision in *Loper Bright* have an impact on the FTC's privacy program?

Kaufman: Well, the short answer is at the moment it won't have a huge impact, but let me back up and actually just talk a little bit about what *Loper Bright* did. So, for 40 years, there was this thing called the Chevron doctrine and what it meant was that if a statute was ambiguous, and to be clear, most statutes are ambiguous, the courts would defer to an agency's reasonable interpretation of that statute. And for a lot of agencies, this has been a major issue. There is been a lot of cases where agencies have relied upon the Chevron doctrine to put forth a reasonable interpretation. The FTC, however, and they've made this point since the case came out, has indicated that, and this is accurate, there have not been many cases out there where the FTC has relied upon the Chevron doctrine to make its points, to bring cases and to defend what it is doing.

So, at the outset, it is not a doctrine that the FTC has relied on heavily, however, and going back to the privacy rulemaking, that will be an area where, to the extent that the FTC comes out with a rule and it gets challenged, had the Chevron doctrine still been in effect, that would be really helpful for the FTC because a court would defer to its interpretation of its authority. Now what will happen is any rule they come out with, it is inevitably going to be challenged and the FTC won't be able to take advantage of that deference that agencies used to have under Chevron and no longer have because of *Loper Bright*. So, although the immediate impact, I don't think is going to be particularly significant on the

FTC, they'll lose that advantage that they had in some of the areas where they're being more creative.

So, I think the rulemaking area is definitely one area where they will feel the impact of it, and I think we may also see that a little bit in some of their more novel unfairness cases. Cases where the FTC might be stretching the bounds of its authority and going at the outer edges of some of their enforcement authority. So, I do think again, it is a doctrine that would have helped the FTC going forward in some of the more creative areas and areas where they might be exceeding their authority just a little bit, but they're not going to be able to take advantage of that anymore and courts will no longer be deferring to them. So, immediately, I don't think it really changes anything, but I think long term, it may help to, or it may actually not help the agency push a more aggressive agenda. So, I think it is an important issue for the FTC but I do think it is more about some of the things that might not be successful going forward based upon it, but I don't think it is changing in any way anything that the FTC is doing on a daily basis today.

Kattman: Thanks so much for joining us today Daniel and Jen.

Kaufman: Amy, thank you so much for having us.

Mitchell: Thank you, Amy. Great speaking with you.

Kattman: If you have any questions for Daniel or Jen, their contact information is in the show notes. As always, thanks for listening to BakerHosts.