UNITED STATES OF AMERICA
Federal Trade Commission
WASHINGTON, D.C. 20580

Office of Commissioner
Alvaro M. Bedoya

# "Who is being left behind?": Enforcement Priorities for a Tech Consumer Protection Agenda

**Prepared Remarks of Commissioner Alvaro M. Bedoya**
**Federal Trade Commission**

**National Association of Attorneys General Presidential Summit:**
**"Consumer Protection 2.0: Tech Threats and Tools"**

**August 9, 2022**

Thank you for that kind introduction. I would like to thank the National Association of Attorneys General for the opportunity to speak with you today. I would like to thank Attorney General Miller for hosting this conference. And I'd also like to *apologize* to him for poaching Max Miller and bringing him to the FTC. Speaking of the Commission, my remarks come with the caveat that I'm speaking for myself, not the full Commission or any of my fellow commissioners. Anyways, it's good to be here.

When it comes to tech, we spend a lot of time thinking about what's changed, what's new, what's different.

How do we protect privacy in virtual reality? How do we protect privacy in a world where machine learning thrives on massive troves of data? How do we protect people when black box algorithms make decisions about their housing, their credit, their health care, their jobs?

Today, I want to resist the urge to focus on the latest implications of the latest technology. I want to take a step back from that leading edge, and instead ask: *Who is being left behind?* And what can we do about it?

I want to talk about three places where I see this happening.

## 1. We need to stop online scams in *all* languages.

Let me start with a personal example.

My wife and I have lived at the same address for years; our names are on the same accounts; we shop in the same places. Like everyone else, we get spam calls, and we get *scam* calls. Yet my wife gets fewer of the calls than I do. I get more of them. And when she asks them to stop, they do. When I ask them to stop, they just keep on calling.

The difference is that my wife gets calls in English. Most of my calls are in Spanish.

This isn't just me. And critically, this pattern is amplified *online*, on the Internet and on social media. Hispanics are more likely to use leading social media and messaging apps than other racial or ethnic groups. We also spend much more *time* on social media as compared to the general population.[1] So, we face a disproportionate share of online fraud.

We're also targeted for *who* we are. For example, after pandemic relief efforts started, Latinos in New York started getting messages promising them $800 of "Christmas help," mimicking messages from a state program to help those left out of other pandemic relief efforts.[2]

So, is there an enforcement gap?

Well, it's hard to find statistics on this, on the levels of online fraud faced by different language communities. But I see this kind of targeting all the time. And if it is this bad for Spanish, the second most spoken language in the country, we can only imagine how things must be for speakers of Mandarin, Tagalog, Vietnamese, Haitian Creole, Amharic, or, critically, speakers of Native American languages, who are disproportionately victimized by scams.[3]

Yet the tools that platforms use to stop scams and fraud are often less effective for languages other than English.

[1] Brooke Auxier & Monica Anderson, *Social Media Use in 2021*, Pew Research Center, Apr. 7, 2021, https://www.pewresearch.org/internet/2021/04/07/social-media-use-in-2021/ (showing Hispanics as more likely to use Instagram, Snapchat, and WhatsApp than white and Black adults, and two percentage points less likely to use Facebook than African-Americans, the most frequent users of that platform); The Nielsen Company, *Descubrimiento Digital: The Online Lives of Latinx Consumers* at 4 (2018), available at https://www.nielsen.com/wp-content/uploads/sites/3/2019/04/the-online-lives-latinx-consumers.pdf ("U.S. Hispanics over-index for the amount of time they spend on social networking sites, with 52% spending 1 or more hour(s) per day (compared with 38% of non-Hispanic Whites) and 24% spending 3 or more hours per day (compared with 13%).").

[2] *In Spanish*: Juliana Jiménez J. & Rommel Ojeda, *Estafadores se aprovechan de los indocumentados: estas son las mentiras más comunes y así puede evitarlas*, Noticias Telemundo, Dec. 15, 2021, available at https://www.telemundo.com/noticias/edicion-noticias-telemundo/inmigracion/estafadores-se-aprovechan-de-los-indocumentados-estas-son-las-trampas-rcna8651; *In English:* Juliana Jiménez J. & Rommel Ojeda, *Scam messages are targeting Latino immigrants. Here's how to avoid them*, NBC News, Dec. 15, 2021, available at https://www.nbcnews.com/news/latino/scam-messages-are-targeting-latino-immigrants-avoid-rcna8861.

[3] Keith B. Anderson, *Consumer Fraud in the United States: An FTC Survey* at ES-4 (2004) available at https://www.ftc.gov/sites/default/files/documents/reports/consumer-fraud-united-states-ftc-survey/040805confraudrpt.pdf (finding that 33.8 percent of American Indians and Alaska Natives surveyed were victims of fraud compared to 6.4 percent for non-Hispanic Whites); Keith B. Anderson, *Consumer Fraud in the United States: The Second Federal Trade Commission Survey* at 27 (2007) available at https://www.ftc.gov/sites/default/files/documents/reports/consumer-fraud-united-states-second-federal-trade-commission-survey-staff-report-federal-trade/fraud.pdf (finding that American Indians and Alaska Natives were 38.6 percent more likely than non-Hispanic Whites to be victims of fraud). *See also* Keith B. Anderson*, Mass-Market Consumer Fraud in The United States: a 2017 Update* at 69-70 (2017), available at https://www.ftc.gov/system/files/documents/reports/mass-market-consumer-fraud-united-states-2017-update/p105502massmarketconsumerfraud2017report.pdf (noting that 23 percent of people surveyed in the "other" category of race and ethnicity, 23 percent of whom identified as American Indians or Alaska Natives and 20 percent of whom were Native Hawaiians or Pacific Islanders, were victims of fraud, higher than any other category). For that reason, the FTC offers some consumer education resources in other languages such as Chinese, Korean, Tagalog, Vietnamese, and Spanish. FTC Consumer Resources in Other Languages at https://consumer.ftc.gov/consumer-resources-other-languages.

For example, one of the many technologies used to detect and stop fraud online is Natural Language Processing,[4] which learns how to interpret language by training on large databases of text. But these models are trained on almost 10 times more English than any other language. When it comes to languages like Cherokee and Diné, that disparity can rise to over *1000 to 1*.[5]

But, critically, this is not *just* a problem about technology. It's also about people—*not having* people. Not having staff that share languages or cultural context with users.[6] Not having experts in the needs of people with disabilities. Not having people from the towns and neighborhoods that are using the products. Without these people, more fraud makes it through.

People talk about algorithmic discrimination as if it's this complex, impenetrable thing. But algorithmic discrimination isn't just about what's under the hood; it's also about having the right mechanic—or simply having *a* mechanic, period.

Unfortunately, platforms have *repeatedly* refused to answer questions from Congress on how many staff they employ to monitor for fraud in languages other than English.[7] That is not okay. That must change.

[4] *See e.g.*, Myle Ott et al., Meta AI, *New advances in natural language processing to better connect people*, Meta, Aug. 14, 2019, https://ai.facebook.com/blog/new-advances-in-natural-language-processing-to-better-connect-people/ ("Natural language understanding (NLU) and language translation are key to a range of important applications, including identifying and removing harmful content at scale..."); Kevin Reece, *Google Maps, Google Maps 101: how contributed content makes a more helpful map*, Google: The Keyword, Feb. 19, 2020, https://www.blog.google/products/maps/google-maps-101-how-contributed-content-makes-maps-helpful/ ("Our machine learning models watch out for specific words and phrases, examine patterns in the types of content an account has contributed in the past, and can detect suspicious review patterns."); Engineering at Meta, *Fighting Abuse @Scale 2019 recap*, Meta, Dec. 13, 2019, https://engineering.fb.com/2019/12/13/security/fighting-abuse-scale-2019/ ("Machine learning (ML) models for detecting integrity issues have made significant progress, thanks to research in natural language processing and computer vision").

[5] *See* Pratik Joshi et al., *The State and Fate of Linguistic Diversity and Inclusion in the NLP World*, Proc. of the 58th Ann. Meeting of the Ass'n for Computational Linguistics 6282, 6284-6285 (2020), available at https://aclanthology.org/2020.acl-main.560.pdf, language appendix available at https://microsoft.github.io/linguisticdiversity/assets/lang2tax.txt (showing databases used for Natural Language Processing contain approximately 1000 times less labeled data in Class 1 languages like Diné (called Navajo in the paper) and Cherokee than English, a Class 5 language.)

[6] At one contractor to a social media company, "everyone who has a remotely Hispanic-sounding name" was reportedly made to "take a Spanish test, and if they failed they were asked to take it again" to provide sufficient Spanish-language staff to monitor the platform. *See* Sarah Emerson, *Facebook's Spanish-Language Moderators Are Calling Their Work A "Nightmare"*, BuzzFeed News, Jan. 13, 2022, https://www.buzzfeednews.com/article/sarahemerson/facebooks-spanish-language-moderators-said-theyre-treated. The same report noted that those fluent in Spanish struggled because the company did not provide a copy of its monitoring guidelines in Spanish for their staff to use.

[7] *See* Office of Senator Ben Ray Luján, *Luján, Klobuchar, Cárdenas Lead Colleagues Urging Tech CEOs to Combat Spanish-Language Disinformation* (2021), available at https://www.lujan.senate.gov/newsroom/press-releases/lujan-klobuchar-cardenas-lead-colleagues-urging-tech-ceos-to-combat-spanish-language-disinformation/, *See also* Facebook, Letter: Facebook's Response to Senator Luján (Aug. 26, 2021), available at https://www.lujan.senate.gov/wp-content/uploads/2021/09/Facebook-Response-Lujan.pdf; Access Now et al., The Santa Clara Principles On Transparency and Accountability in Content (2021), available at https://santaclaraprinciples.com.

But I'm not here to just point a finger at industry. Because from everything I know, this problem extends across civil law enforcement, including federal law enforcement.

Law enforcement does not have a language exception. It is our duty to protect you no matter what language you speak. Particularly if fraudsters target you because it's harder for us to protect you. Yet we do not have the tools we need to systematically identify and stop these kinds of frauds. People are being left behind.

So, when I meet with platform companies, I'm going to ask: What tools are you using to identify fraud in all languages, particularly Native American ones. What are you doing about bias?

But algorithmic bias is just the start of the conversation. I'm also going to ask companies about the *people* they're hiring. Who is building these systems? Who runs them? Who maintains them? How many people do you have monitoring for fraud across languages? Do they have the resources they need?

I'm asking similar questions at the Federal Trade Commission.

Thankfully, the Commission has a bipartisan history of trying to get ahead of this problem. Twenty years ago, Republican Chairman Tim Muris led an effort to systematically reach out to Spanish-language media to put out fraud alerts and to staff up accordingly.

More recently, in 2014, Democratic Chair Edith Ramirez—the first Latina FTC commissioner in a century—established the Every Community Initiative to build upon this work and address disparities affecting communities of color.

Thanks to the relentless work of FTC staff, the vision of these two chairs has been made an everyday reality. But there is still work to be done.

I am already working with the Every Community team to identify strengths, gaps, best practices, and resource needs. We will not be able to get this done without resources.

## 2. <u>We need to protect teen mental health online.</u>

We have to make sure that the language you speak does not make you more vulnerable to fraud online. We also have to make sure that we account for the fact that life online may affect people differently depending on where they are in life, or how old they are.

When people raise concerns about the online attention economy, industry often responds with: 'What's the harm?'

'Yes, we track people. Yes, we use various techniques to *keep* people online. But people just get more of what they want. Who exactly is getting hurt?'

Our keynote speaker today, Frances Haugen, might say that teenagers, particularly teenage girls, are getting hurt. She is not alone in sounding this alarm. Congressional hearings, academic research, media reporting and individual stories from families are forcing questions about how social media affects children and teens' mental health.

Indeed, a growing body of evidence suggests that teenagers, particularly teenage girls, who spend more than two or three hours a day on social media, suffer from increased rates of depression, anxiety, and thoughts of suicide and self-harm.

One paper explained that "adolescents using electronic devices 3 or more hours a day were 34% more likely to have at least one suicide-related outcome than those using devices 2 or fewer hours a day…"[8]

Another paper described "[d]aily [social networking site] use of more than 2 hours was… independently associated with poor self-rating of mental health and experiences of high levels of psychological distress and suicidal ideation."[9]

Another study found that "[g]reater social media use [was] related to online harassment, poor sleep, low self-esteem, and poor body image."[10] By and large, the research on this subject suggests that this association between social media use and depressive symptoms is larger for girls than for boys.[11]

Now, we need to avoid moral panic. So I want to be accurate and precise.

Some of these are longitudinal studies that track people over time and are better at establishing causation. Others are cross-sectional studies that only deal with correlation, and that *openly ask* if there's a two-way relationship between social media use and mental health issues, where each increases the other.[12] And there is well-regarded peer-reviewed research which suggests that the relationship is one of correlation, not causation, and a small one at that.[13]

[8] Jean M. Twenge et al., *Increases in Depressive Symptoms, Suicide-Related Outcomes, and Suicide Rates Among U.S. Adolescents After 2010 and Links to Increased New Media Screen Time*, 6 Clinical Psychological Science 1, 3, 10 (Jan. 2018), available at https://doi.org/10.1177/2167702617723376.

[9] Hugues Sampasa-Kanyiga & Rosamund Lewis, *Frequent use of social networking sites is associated with poor psychological functioning among children and adolescents*, 18(7) Cyberpsychology, Behavior, and Social Networking 380 (Jul. 2015), available at https://www.researchgate.net/publication/280059931_Frequent_Use_of_Social_Networking_Sites_Is_Associated_with_Poor_Psychological_Functioning_Among_Children_and_Adolescents.

[10] Yvonne Kelly et al., *Social Media Use and Adolescent Mental Health: Findings from the UK Millennium Cohort Study*, 6 EClinical Medicine 59, 59 (2018), available at https://www.thelancet.com/action/showPdf?pii=S2589-5370%2818%2930060-9.

[11] *See, e.g., ibid*.

[12] *See* Sarah Coyne et al., *Suicide Risk in Emerging Adulthood: Associations with Screen Time over 10 years*, 50 Journal of Youth and Adolescence 2324, 2324 (2021), available at https://doi.org/10.1007/s10964-020-01389-6 (the longest longitudinal study to date on this subject); s*ee also* Sampasa-Kanyiga & Lewis *supra* note 9 (speculating about two-way relationship between depression and social media use).

[13] *See* Amy Orban & Andrew K. Przybylski, *The association between adolescent well-being and digital technology use*, 3 Nature Human Behaviour 173 (Feb. 2019), available at https://www.nature.com/articles/s41562-018-0506-1; Noah Kreski et al., *Social Media Use and Depressive Symptoms Among United States*

My point is this: Our time on social media, as adults, may affect us differently than it does young people. And while we may not know exactly what this effect is, there is enough here that we need to know more. And once we account for the fact that kids' screen time is increasing most for low-income kids and kids of color, we have even more reason to dig deeper.[14]

And so, when we meet with social media and messaging companies, we need to ask them: What exactly do you do to keep children and teenagers online? Not just up to age 12—all teenagers. Why are you using these techniques? What do you know about how it affects kids and teens? And what are you doing to prevent harm?

And we need to ask ourselves if we have the people and data to study this problem adequately. In 2009, the Federal Trade Commission hired its first staff technologist—a computer scientist named Chris Soghoian. Since then, we have hosted luminaries like Latanya Sweeney, Ashkan Soltani, Lorrie Cranor, Ed Felten, among others. These experts help us understand complicated technologies.

We need another update. One of the best ideas in the modern tech debate that has received way too little attention is a proposal from Representative Cathy McMorris Rodgers, a Republican of Washington. She proposed that in addition to staffing up the Federal Trade Commission with technologists, it should also be staffed with *psychologists* and youth development experts.[15]

I'm thrilled that this proposal is part of the bipartisan privacy bill currently working its way through Congress.[16]

I will add that Commissioner Christine Wilson, my friend and Republican colleague, shares my concerns in this area. And in addition to studying these bills, we are looking at other constructive steps we can take to advance research, heighten awareness, and protect children online.

### 3. **<u>We need to protect location data.</u>**

So far, I've focused on making sure we don't leave people behind based on the language they speak, or how old they are. We also need to update our privacy laws so that they don't leave people behind. I'm focused in particular on location data, also known as "geolocation."

*Adolescents*, 68 Journal of Adolescent Health 572 (2021), available at https://www.jahonline.org/action/showPdf?pii=S1054-139X%2820%2930403-1; Michaeline Jensen et al., *Young Adolescents' Digital Technology Use and Mental Health Symptoms: Little Evidence of Longitudinal or Daily Linkages*, 7(6) Clinical Psychological Science 1416 (2021), available at https://journals.sagepub.com/doi/10.1177/2167702619859336.

[14] Melinda Wenner Moyer, *Kids as Young as 8 Are Using Social Media More Than Ever, Study Finds*, The New York Times, Mar. 24, 2022, https://www.nytimes.com/2022/03/24/well/family/child-social-media-use.html.

[15] Control Our Data Act, H.R. __ [Discussion Draft], 117th Cong. § 114(b)(2)(D) (2021) available at https://republicans-energycommerce.house.gov/wp-content/uploads/2021/11/2021.11.02-Republican-CODA-Draft-.pdf.

[16] American Data Privacy and Protection Act, H.R. 8152, 117th Cong. § 205(d)(4) (2022) available at https://www.congress.gov/bill/117th-congress/house-bill/8152/text.

When I was a young Senate staffer, I helped organize a hearing to look at how powerful Internet companies were collecting, protecting, and sharing data on our movements.

Right after we announced that hearing, my boss, Senator Franken, got a message from the Minnesota Coalition for Battered Women. They said that the moment someone arrived at one of their shelters, one of the first things that staff did was shut down her cellphone. They explained that many of their clients were tracked through so-called "stalking apps" that let their abusers follow them, in secret, in real-time.[17]

They shared the story of a woman in St. Louis County, Minnesota, who fled her abuser and went to a domestic violence program located in a county building. Five minutes after walking in, she got a text asking her: Why are you at the county building?

She was terrified, so she went to the courthouse to get an order of protection. And then she got another text message asking her: Why are you at the courthouse? Are you getting a restraining order?

All of that happened through a stalking app.

That was 2011. Since 2012, the Federal Trade Commission has identified certain kinds of data so sensitive that they must only be obtained through "affirmative express consent." These include children's data, financial and health information, Social Security numbers, and certain geolocation data.[18]

Well, Congress has passed laws protecting children's data, financial information, health information, and your Social Security number. It has passed no such law for location data.

And so, over a decade after I first spoke with those domestic violence advocates, in 2022, our geolocation technology is not under control. There is a large, unregulated market for this data. If you are in an abusive relationship, if you are a victim of stalking, then your inability to protect this data is a real threat to your safety. [19]

But it is now so much worse than that. Today, this lack of privacy threatens people who want to have private lives without their employer finding out and firing them.[20] It threatens servicemembers stationed abroad who want to use fitness apps but who do not realize that those

[17] *Protecting Mobile Privacy: Your Smartphones, Tablets, Cell Phones and Your Privacy: Hearing Before the Subcomm. on Privacy, Technology, and the Law of the S. Comm. On the Judiciary*, 112th Cong. 401-407 (2011), available at https://www.judiciary.senate.gov/imo/media/doc/CHRG-112shrg86775.pdf (testimony of The National Network to End Domestic Violence with The Minnesota Coalition for Battered Women).

[18] FTC Final Report, Protecting Consumer Privacy in an Era of Rapid Change at 47 and n214 (2012), available at https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf.

[19] Coalition Against Stalkerware, *Annual Kaspersky report on stalkerware highlights the link between online and offline violence* (Apr. 12, 2022), available at https://stopstalkerware.org/news/.

[20] Associated Press, *Priest outed via Grindr app highlights rampant data tracking*, NBC News, Jul. 22, 2021, https://www.nbcnews.com/tech/security/priest-outed-grindr-app-highlights-rampant-data-tracking-rcna1493.

apps broadcast their location to the public and to our adversaries.[21] And now, a lack of location privacy also threatens people who must make deeply private choices about their bodies and their families.

So, what do we do?

I think that *any* company that collects, retains, or uses location data should think hard about how to better protect their users. Because I'll be asking those companies: Does the collection need to happen at all? Why and how are you using that data? What more can you be doing to protect your users?

There are various federal laws that govern the collection, use, and sharing of location data or other sensitive user data. These include the FTC Act, the Safeguards Rule, the FCRA, the Health Breach Notification Rule, and the Children's Online Privacy Protection Rule.[22]

I will do everything in my power to ensure that these laws are enforced rigorously. Many of you can enforce similar and at times overlapping state laws. I urge you to prioritize their enforcement.

* * *

There will always be a new technology. There will always be a new application of that technology. We need to spend time at that leading edge. My hope is that we spend just as much time trying to help the people trailing behind.

Thank you for your time. I'd be glad to hear your thoughts and answer any questions.

[21] Jeremy Hsu, *The Strava Heat Map and the End of Secrets*, Wired, Jan. 29, 2010, https://www.wired.com/story/strava-heat-map-military-bases-fitness-trackers-privacy/.

[22] Kristin Cohen, *Location, health, and other sensitive information: FTC committed to fully enforcing the law against illegal use and sharing of highly sensitive data¸* FTC Business Blog (Jul. 11, 2022), available at https://www.ftc.gov/business-guidance/blog/2022/07/location-health-other-sensitive-information-ftc-committed-fully-enforcing-law-against-illegal-use ("The marketplace for this information is opaque and once a company has collected it, consumers often have no idea who has it or what's being done with it. After it's collected from a consumer, data enters a vast and intricate sales floor frequented by numerous buyers, sellers, and sharers").