

**BEFORE THE SENATE COMMITTEE ON COMMERCE,  
SCIENCE AND TRANSPORTATION**

**HEARING ON PROTECTING CONSUMER PRIVACY**

**TESTIMONY OF ASHKAN SOLTANI  
INDEPENDENT TECHNOLOGIST**

September 29, 2021

Dear Chair Cantwell, Ranking Member Wicker, and Members of the Committee:

Thank you for inviting me here today to testify before you. My name is Ashkan Soltani. I am a researcher and technologist, and formerly served as the Chief Technologist at the Federal Trade Commission (FTC or Commission).

Since departing the FTC, I've helped support state-level privacy and tech enforcement, both directly as an expert, and through my involvement with Georgetown Law, where I am a Distinguished Fellow at both the Institute for Technology Law & Policy and the Center on Privacy and Technology. I also helped author California's landmark privacy laws, the California Consumer Privacy Act (CCPA) and the California Privacy Rights Act (CPRA). I have seen firsthand the challenges in bringing cases against technology companies and making new laws to constrain bad behavior.

Today, I'd like to discuss why the FTC needs expanded authority to handle data and technology matters, how to appropriately expand the Commission's staff and talent pool, and why it is important that any new bureau have a specific mandate to investigate new technologies and harmful data practices that pervade the modern digital ecosystem.

### **Expanding FTC Authority**

I'm pleased to be invited as Congress and this Committee are considering significant changes to the structure and funding of the Federal Trade Commission. The proposal to create and fund a new bureau at the FTC—which Chair Cantwell also called for in S. 2968, the Consumer Privacy Rights Act—is a strong step forward towards providing the Commission with the resources it needs to effectively protect consumers in the digital economy. A new bureau focused on technology and data protection would help the FTC support its mission of policing unfair and deceptive practices related to privacy, data security, identity theft, and data abuses. I strongly support it.

First and foremost, in addition to more resources, the agency desperately needs additional legal authority to meet the new challenges of the digital economy. With the exception of a few sectoral laws, such as the Children's Online Privacy Protection Act (COPPA) or the Fair Credit Reporting Act (FCRA) there is no comprehensive federal privacy regime in the United States. We're long overdue for a change.

Many of the digital harms from the surveillance economy are monitored through the FTC's enforcement of deceptive practices under Section 5 of the FTC Act. But this framework does not effectively protect consumers. For example, consumers often don't directly interact with the hundreds of data brokers that surreptitiously collect their data as they move about their digital lives. This ecosystem makes the required "notice" component of a deception case difficult to prove. Unfairness authority is hard to use to enforce privacy harms, since the courts have not

typically recognized privacy harms as cognizable injuries under FTC unfairness standards. Moreover, the FTC lacks the authority to issue civil penalties for first-time violations.

While expanding the Commission's budget is a great step, Congress should complement that funding with additional privacy authority so the agency can properly fulfill its mission. That's why it is critical that Congress passes federal privacy legislation that builds upon, but does not preempt, privacy legislation adopted in states like California and Colorado. Already, there has been a concerted effort in Congress and in statehouses across the nation to muddy the conversation and introduce privacy bills that appear strong, but merely entrench the status quo of privacy violations. Specifically, bills like the one adopted in Virginia appear robust, but allow exploitative business practices to continue unabated.

This legislation, drafted by industry and passed with little debate, seeks to confuse the conversation and provide cover for deep-pocketed groups to change the conversation from one about strong protections for consumers to one about “harmonizing” protections. But these bills represent a race to the bottom, and are often deeply flawed. For instance, the Virginia bill includes problematic technical definitions of personal information, which exclude nearly all of the ad tech industry from its scope of opt-out. Under this law, it is not clear that the state will allow consumers to opt out of cross-contextual targeted advertising, the tracking of individuals across unaffiliated websites and services. Any law passed by Congress should build upon the work done by states that does protect their consumers, and not preempt state laws that seek to provide additional protections to those enacted by Congress.

Congress should give the Federal Trade Commission a legal mandate to enforce privacy laws beyond those bad actions that are deceptive or unfair. This is doubly true since—for certain historical reasons—the Commission rarely initiates privacy cases under its unfairness authority. The agency's existing authority to regulate privacy, in practice, limits it to taking action only after a company has made an explicit promise to consumers and then broken that promise. This is well short of the robust protections necessary to ensure the privacy and security of consumers' data.

Strong FTC enforcement authority, such as measures proposed by many members of this Committee, is essential, as are the provisions granting the state attorneys general and private consumers the authority to bring suit. Together, they would enable the Commission to undertake a robust enforcement regime, and empower consumers and state law enforcement to step in when the Commission cannot or will not do so.

## Expanding FTC Capacity

### *The Agency Currently Has Few Privacy Staffers*

Expanding the agency's capacity to enforce the law is also critical. Laws alone without enforcement don't protect the public. Presently, the Commission's Division of Privacy and Identity Protection (DPIP) is tasked with solving the nation's myriad privacy and cybersecurity issues with a bare-bones staff of about 40 attorneys and a handful of technologists. In comparison, European countries have robust laws, such as the General Data Protection Regulation (GDPR). Each country typically has a Data Protection Agency (DPA) with hundreds of staff and dozens, if not hundreds of technologists. For example, the German DPA has 745 staff and nearly 100 tech experts enforcing their law for a country with one quarter the population of the United States.<sup>1</sup> Similarly, France, which has one-fifth our population, employs nearly 200 staff, including 30 tech experts. The nations that employ the most technologists have had the most success in bringing corrective actions against big technology companies.<sup>2</sup>

The FTC, with its 40 staff and fewer than 10 technologists, simply does not have enough resources to police an industry that touches nearly every aspect of the American economy. This leads the agency to prioritize certain cases, and ignore privacy violations if they aren't deemed sufficiently harmful or easy to prosecute, or if the staff hours aren't available. If staff are already engaged in one privacy or security matter, they may simply ignore harmful acts that arise while they are occupied.

The problem is exacerbated when businesses choose to litigate a case rather than accept a settlement. By some accounts, these cases can occupy one-third to half of the Commission's entire privacy division on a single matter. Again, that's half of the entire federal privacy staff working on one case for years, at the exclusion of other critical work. Businesses and their lawyers know and exploit this: in my experience, when outside counsel knows that the Commission has its hands full with litigation, they recommend that their clients take aggressive stances in response to FTC action, knowing that the FTC is unlikely to have the resources to adequately challenge them. Companies seek this expert knowledge, and hire former FTC officials to advise them on how to best avoid regulatory and enforcement scrutiny. Overworked commission staff have a hard time making up for this level of deliberate gamesmanship, and businesses' strategies to avoid FTC enforcement are quite successful.

### *The FTC Has Limited Enforcement Staff to Monitor Compliance*

The FTC also does not have enough enforcement staff to monitor compliance with their orders. The Division of Enforcement—which is separate from DPIP, which investigates privacy

---

<sup>1</sup> Irish Council for Civil Liberties, *Europe's Enforcement Paralysis* 10 (2021), <https://www.iccl.ie/wp-content/uploads/2021/09/Europes-enforcement-paralysis-2021-ICCL-report-on-GDPR-enforcement.pdf>.

<sup>2</sup> *Id.* at 7 (noting that Germany has taken 16 and France 19 corrective actions versus two or three actions taken on average by every other member state).

violations—is tasked with overseeing compliance with *all* of the Commission’s consent decrees, in addition to the myriad of laws relating to Made In USA and textile labeling, for example.<sup>3</sup> The same lawyers who ensure that social media companies have robust privacy and data security programs are making sure labels on bed linens are correct. Technology enforcement requires its own nuanced set of skills, and the FTC needs both numbers and staff with special knowledge. Current enforcement staff have varying skill sets, and while they may be generalists, they may well not understand algorithms, APIs, or data encryption.

The Commission needs not only enough staff to monitor compliance with their orders, it needs that staff to have the expertise to understand the complex technological principles the initial violation was based on. Presently, the staff who investigate and bring a matter are not the ones who handle enforcement of consent decrees for those matters. The staff disconnect often results in a huge gap in expertise and understanding regarding what underlying privacy violations occurred. Ideally, the Commission should have enough staff to leverage the expertise of the initial investigators as part of the enforcement oversight process.

In fact, many of the “Big Tech” companies with which Congress is presently concerned—such as Facebook, Apple, Google, and others—are already under consent decree with the Commission. The companies have already taken some action that has landed them—essentially—under probation with the Commission, and have agreed to a set of negotiated terms with the agency. While this appears reasonable on paper, these orders don’t do much to curb problematic practices: staff limitations at the agency mean that enforcement is lax or non-existent. For instance, one common enforcement tool is to require companies to submit regular third-party assessments of their data practices. These third-party assessments can provide the Commission insight into ongoing compliance by the company. But these assessments are only made available to the FTC upon request, and the Commission staff rarely has time to request them. In fact, one former FTC enforcement staff has publicly stated that the FTC rarely even reads these assessments.<sup>4</sup>

Under the current arrangements at the FTC, it is quite possible—even likely—that at least some of the companies under order are violating the terms of their agreement but that the Commission doesn't have the adequate resources to properly investigate.

### *The FTC Has Limited Technologists on Staff*

In 2010, I was one of the first two technologists ever hired by the Federal Trade Commission to work on privacy matters in DPIP. My workload quickly went from handling small portions of matters to being deeply involved in nearly every case brought by the Commission. I personally helped to bring the Commission's first major successful cases against Twitter, Google, and

---

<sup>3</sup> Federal Trade Commission, *What We Do*, <https://www.ftc.gov/about-ftc/what-we-do/enforcement-authority>.

<sup>4</sup> Megan Gray, *Understanding and Improving Privacy ‘Audits’ Under FTC Orders* (2018), [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=3165143](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3165143).

Facebook. I have firsthand experience with how important technologists are to the effective oversight of big technology companies.<sup>5</sup>

Despite this, the Commission only has a limited number of technology experts on staff. When I re-joined the agency in 2014, as Chief Technology Officer, there was only one other technologist on staff. With the support of the then-Chair Ramirez, I helped to create the Office of Technology Research and Investigation (OTech) and grew that number of technologists to approximately ten by the end of my term in 2016. But due to political pressures, these technologists were housed not as a separate division that could serve the entire agency, but instead in an obscure business unit within the IT staff of the Bureau of Consumer Protection (BCP): the same group that maintains eDiscovery computers and other litigation support resources for the Commission. This awkward structure, which is in place to this day, effectively restricts the team by limiting their ability to report to key decision makers, and restricts them to functioning alongside the same group that provides IT support to investigators, dramatically reducing technologists influence across key investigations and policymaking.

Additionally, staff technologists frequently recuse themselves from active matters at the Commission due to the FTC's overly broad interpretation of rules prohibiting technologists from **ever** working on matters in which they participated during their employment at the Commission. Because of the unique nature of technologists' work, this same restriction does not apply to the attorneys or economists at the Commission, effectively penalizing technologists who work for the FTC. This overly broad provision intended to bar technologists from seeking post-FTC employment at many private companies on the same matters also prohibits them from working alongside the FTC in civil enforcement at state agencies, including, as was my experience, for the offices of state attorneys general.<sup>6</sup>

Even in its hobbled structure, OTech was able to help support the Commission's staff by providing trainings on emerging technology issues, giving briefings on topics as varied as "advertising industry market dynamics, online manipulation, creepware apps, misuse of payment data from web skimming, methods of detecting deepfakes and authenticating original media, and using mobile phone data to inform COVID-19 public health response," according to their budget justification for 2022.<sup>7</sup> Expanding the role and influence of this group will greatly aid consumer protection efforts by the Commission on key topics of interest to Congress

---

<sup>5</sup> See also, Matt Burgess, *How France Tamed Google*, Wired (Aug. 2, 2021), <https://www.wired.co.uk/article/google-france-fines> (explaining that the success of the major French antitrust case against Google was due to the agency relying on technologists, rather than lawyers, to build the case).

<sup>6</sup> Lindsey Barrett, Laura Moy, Paul Ohm & Ashkan Soltani, *Illusory Conflicts: Post-Employment Clearance Procedures and the FTC's Technological Expertise*, 35 Berkeley Tech. L. J. 793 (2020), [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=3895823](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3895823).

<sup>7</sup> Federal Trade Commission, Congressional Budget Justification Fiscal Year 2022 at 63. <https://www.ftc.gov/system/files/documents/reports/fy-2022-congressional-budget-justification/fy22cbj.pdf>.

## Creating a New FTC Bureau

### *Incentivizing Collaboration and Efficiency at the FTC*

Providing additional resources to the FTC is an essential first step to empowering the Commission to pursue strong technology enforcement. A new bureau, funded fully, will ensure that the Commission can fulfill its mission, and I support the measure. However, it is essential that the creation of a new bureau enables the Commission to collaborate and leverage its resources to investigate fully the wide range of harms caused by new technology and data practices.

To ensure that funding and additional resources are most effective, Congress should make clear that collaboration between all of the bureaus is an important goal of its funding. Too often, the bureaus at the FTC work in isolation, creating silos that fail to maximize the expertise throughout the Commission. For example, BCP houses the Division of Marketing Practices (which investigates fraud), the Division of Advertising Practices (investigating influencers and major advertising practices), and the Division of Privacy and Identity Protection (investigating privacy and identity theft). These three divisions often look into the same entities for related matters, but do not often collaborate across the divisions.

Under this structure, cases that deal with financial practices issues in one division could miss the digital harms that pervade the business practices at issue. Fortunately, there appears to have been cross-division collaboration in a recent Financial Practices case: Venmo -- likely due to technology staff who are better able to move between these boundaries. But in my experience, cross-division collaboration is unfortunately not the norm which creates inefficiencies and challenges when investigating fast-moving and well resourced industry players.

### *Technology and Data Protection: A New Bureau By Any Other Name*

One way to incentivize collaboration and forward-looking enforcement is to appropriately scope any new bureau to reflect the underlying needs of the current digital ecosystem. Data security, data abuse, and identity theft all have one thing in common: technology and the underlying data they rely on. Narrowly constraining a new bureau on solely one of those practices, privacy, and giving it a name that reflects that narrow focus, would fall short of the consumer protection goals laid out for the FTC and by Congress. Instead, the bureau's mission and name should reflect the realities of current challenges: The Bureau of Technology and Data Protection.

This may seem like a small point, but names do matter. Many of the harms that concern this Committee and are investigated by the Commission do not fall neatly into the category of "privacy" harms. Instead, many are abuses of personal data, harms to civil rights or liberties, abuses of kids' data that fall outside of COPPA, and the intentional design and release of

harmful products.<sup>8</sup> Data firms often innovate new ways to track or identify users without consent, and cannot easily be cabined by a singular focus on “privacy.”<sup>9</sup> Other harms, such as algorithmic bias or hyper-targeted news feeds and recommendation algorithms, also do not fit neatly into “privacy” as a category. A new bureau should be empowered to investigate these data practices: their disproportionate effects on minorities and other vulnerable populations, are often what harm consumers the most, and often do not fall squarely into “privacy.”

I have long advocated for the creation of a new Bureau of Technology and Data Protection, because technology and *data* pervades nearly every case that comes before the Commission. Congress should create a bureau with the mission and expertise to investigate harmful practices across the technology ecosystem and support the existing divisions—like the Division of Privacy and Identity Protection, Ad Practices, and Marketing Practices—in order to better protect vulnerable populations. This Bureau of Technology and Data Protection could issue guidance to staff about how to approach technology in matters and could support investigations across the entire range of digital harms the commission addresses.

A Bureau of Technology and Data Protection would provide a “hub” of resources for the Commission that would serve across the agency’s many consumer protection missions, incentivize collaboration across agency divisions, and encourage efficiency. The Commission could look to the Bureau of Economics (BE) as a model. Similarly to BE, the new bureau should perform research and investigations to help support the Commission’s mission. The new bureau can also function as a community of practice and expertise within the Commission that informs other divisions and the FTC as a whole. When necessary, employees of the new bureau, including technologists and other experts, could be detailed to other bureaus or groups to support ongoing matters that may benefit from their expertise. These meaningful opportunities for collaboration and education will create a more robust culture within the FTC, and help draw talent.

The FTC needs more resources, but it also needs the right resources. Narrowly focusing the bureau’s expertise on “privacy,” rather than a broader mission of data practices generally, would create structural limitations that will live on in the Commission for years to come.

## **Recommendations**

I’d like to briefly lay out a few concrete recommendations for this Committee to consider as it moves forward on privacy legislation, either in this current legislation or later.

First, this Committee should focus on the outcomes it seeks to enable, rather than becoming entangled in the details of agency organization. While additional resources and bureaus are

---

<sup>8</sup> K.G. Orphanides, *Children’s YouTube Is Still Churning Out Blood, Suicide and Cannibalism*, *Wired* (Mar. 23, 2018), <https://www.wired.co.uk/article/youtube-for-kids-videos-problems-algorithm-recommend>.

<sup>9</sup> See, e.g., Geoffrey A. Hunter & Tatum Fowler, *When You ‘Ask App Not to Track,’ Some iPhone Apps Keep Snooping Anyway*, *Wash. Post* (Sept. 23, 2021), <https://www.washingtonpost.com/technology/2021/09/23/iphone-tracking/>.



important, it is important to implement change in ways that avoid bureaucratic siloing or creating divisions between staff at the agency that may well be counterproductive to ensuring a strong privacy enforcement regime. Instead, the Committee should focus on creating incentives and resources for the agency to hire experts and seek collaborative solutions to continuing market problems.

For instance, many of the most pressing harms this Committee is concerned with, such as the psychological harms caused to teens by social media,<sup>10</sup> do not fit cleanly into existing privacy enforcement tools. The Committee should seek to enable the Commission to seek remedies for digital conduct that causes harm, even when the practice doesn't fall neatly under deceptive or unfair practices. Additional enforcement authorities, such as enabling the Commission to protect against negligent design or abusive business practices, would go a long way to protecting consumers in the digital age.

This Committee could address these harms by providing guidance to the Commission with the funding of this Bureau. For instance, by directing the Commission to conduct a rulemaking to reduce the instances of identity theft or ransomware attacks online, to increase safeguards around extractive data practices (such as microtargeting), or to protect populations that are particularly vulnerable online, such as communities of color, the LGBTQ+ community, women, and children.

Similarly, the Committee could greatly reduce the burden on consumers by directing the FTC, as Senator Blumenthal already has,<sup>11</sup> to adopt a Global Privacy Control (GPC) as a legally adequate opt-out mechanism.

Alongside additional funding and Congressional direction, the Committee should take steps to ensure that the Commission hires a wide range of staff outside its traditional lawyers, economists, and technologists. In addition to those professionals, the agency should hire statisticians, designers, social scientists and behavioral researchers, such as experts on child development, who can guide complex cases that come before them. These experts would allow the FTC to review product documents at their earliest stages, understand complex project calculations, and identify manipulative designs. Additional expertise will also help the agency identify the current business practices and apps might contravene existing Section 5 authority and empower the agency to more fully use its existing enforcement tools.

Further, the Commission should devote more energy to developing and retaining its talent outside the traditional Washington, DC pool. It should take steps to hire talented individuals from across the country, not just Washington. The pandemic showed that remote work is possible,

---

<sup>10</sup> Georgia Wells, Jeff Horowitz & Deepa Seetharaman, *Facebook Knows Instagram Is Toxic for Teen Girls, Company Documents Show*, Wall St. J. (Sept. 14, 2021), <https://www.wsj.com/articles/facebook-knows-instagram-is-toxic-for-teen-girls-company-documents-show-11631620739>.

<sup>11</sup> Letter from Senator Blumenthal, Senator, to FTC Chair Lina Khan (Sept. 20, 2021), <https://www.blumenthal.senate.gov/imo/media/doc/2021.09.20%20-%20FTC%20-%20Privacy%20Rulemaking.pdf>.

and in many circumstances desirable; hiring nationwide, to remote positions, and in the regional offices, would better enable the Commission to compete for talent with the firms it oversees.

Once the Commission has talent in the door, it needs to do a better job of retaining it. Technologists' pay should be raised to be more competitive with technology salaries, which are often many times higher than what the Commission offers. Technologists also need to be able to complete meaningful and engaging work at the Commission without worry that the FTC's obtuse conflicts rules will prevent them from seeking future employment later in their careers. Congress should seek answers from the FTC about how the Commission will clarify and update its conflict rules in order to better attract technologist talent.<sup>12</sup>

## **Conclusion**

The creation of a new bureau at the Commission would be an important step forward, but it is not the only important change that is needed, and the work can't stop there. With a new bureau, the United States will gain a stronger federal Data Protection enforcer, which will help allay concerns from Europe, and keep us competitive on a global scale.

The new bureau needs not just money, however, but additional substantive authority to investigate and curtail harmful data practices and to rely on Commission resources. These necessary tools include straightforward legislative fixes, such as providing the Commission with first-time civil penalty authority. As the Committee continues to pursue this matter, it should strongly prioritize drafting and passing a comprehensive data privacy law that empowers federal regulators, including the FTC.

Congress should consider meaningful protections for consumers, including strengthening the Commission, ensuring the attraction and retention of talented federal staff, and ensuring that there are robust laws on the books to protect American consumers.

---

<sup>12</sup> Lindsey Barrett, Laura Moy, Paul Ohm & Ashkan Soltani, *Illusory Conflicts: Post-Employment Clearance Procedures and the FTC's Technological Expertise*, 35 Berkeley Tech. L. J. 793, 826 (2020), [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=3895823](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3895823).