U.S. Senator Maria Cantwell

U.S. Senate Committee on Commerce, Science, and Transportation Hearing Titled, "Protecting Consumer Privacy."

Witnesses: David Vladeck, Professor and Faculty Director the Center on Privacy and Technology, Georgetown Law and former Director of the Federal Trade Commission Bureau of Consumer Protection; Morgan Reed, President, The App Association; Maureen Ohlhausen, Partner and Section Chair (Antitrust & Competition Law), Baker Botts, and former Acting Chairman of the Federal Trade Commission; Ashkan Soltani, Independent Researcher and Technologist and former Chief Technologist of the Federal Trade Commission

September 29, 2021

Opening Statement

[AUDIO] [VIDEO]

Cantwell: Good Morning. Today we are having a hearing on "Protecting Consumer Privacy," and we will hear from a panel of experts, three of whom have previously been on the front lines of fighting to protect consumer privacy, at the primary agency charged with protecting consumers' privacy and data security, the Federal Trade Commission.

We all know the challenges of the information age, and they've brought us new products and services. But it has also exposed and threatened consumer privacy by unnecessarily collecting, storing, selling, and exposing consumers' most personal data to theft and harm.

Every year, for the past five years, more than 140 million people have been affected by data breaches exposing their personal data to thieves and fraudsters. And from July 2019 through July 2020, more than 650,000 residents of my state, Washington, were victims of data breaches, including the release of their healthcare information, banking records, social security numbers, and credit card information.

Last week, it was reported that last May, Simon Eye's chain of optometry clinics had been data breached exposing 144,000 individuals' sensitive medical data. This past April the personal data of over 500 million Facebook users, including phone numbers, full names, locations, and email addresses, were posted in a hacking forum. 32 million records were from the United States, providing key information with people who would want to use those in various ways. And last June, Volkswagen announced a data breach and exposed phone numbers and email addresses of 3.1 million Americans who had shopped for cars.

So it isn't a surprise that all this data being stolen and exposed, that more people have become victims of identity theft. Identity Theft complaints have increased 375% between 2017 and

2020. The harms are causing real damage to consumers. According to a May 2021 report by the Identity Theft Resource Center, victims of identity theft are turned down for loans, unable to rent houses, they have their credit damaged, they are billed for medical services they never received, and they can't find unemployment benefits because their name was basically stolen.

Our precise locations, fitness regimens, computer strokes, and even our friends and family networks have basically been turned into commodities. We know that recently, The Wall Street Journal also found that even after you turn off some of your app tracking on your iPhone, iPhone apps can continue to track you using your device fingerprints. The fact is that companies collecting this information are not doing enough to safeguarding information that they collect or keep their privacy promises. Unfortunately, the Federal Trade Commission which is tasked with preventing consumer data abuses has not been given the resources to keep pace with this tech based economy.

Professor Vladeck, we will hear from you, but I think you have in your opening remarks that basically now the FTC's docket is dominated by these technology issues. The truth is that our economy has changed significantly and the Federal Trade Commission has neither the adequate resources, nor the technological expertise at the FTC to adequately protect consumers from harm.

While the commission is responsible for keeping up with the latest technology companies in the world, according to today's testimony, quote, "It has fewer than 10 employees on staff with the right technology expertise," end quote. The FTC simply does not have the tools to fend off privacy attacks, data breaches, internet scams, and ransomware digital abuses that threaten consumers and our economy. It's not to say the FTC hasn't done some good work. But when we look at the volume of what we're facing, it's clear they're under resourced.

Even where the FTC has taken enforcement actions against companies, the companies continue to violate those FTC orders, which is beyond frustrating. Even though the FTC has been able to use their current authority of unfair and deceptive practices, companies like Facebook or others may gladly pay a $5 billion fine, when actually, they can still make over $70 billion a year from some of these same practices.

So compliance, we need compliance. Compliance with existing laws, or compliance with new rulemaking, or compliance with the new privacy law will be insufficient if the FTC is not well resourced, technology sophisticated, and the policeman on the beat of the information age.

The U.S. Department of Commerce estimated that the digital economy accounted for 9.6% of GDP in 2019 and it grows annually at a rate of 5.2%. This means we're just going to continue to be ever dependent on this economy. I'm not even going to spend time talking about it at length, the great effect of state actors attacking our systems. The fact that consumers are left vulnerable to these events. But the economy of today is that the digital economy generates $2 trillion annually. So it will continue to be a target.

As the economy grows, the volume of data collected about Americans, and the amount of data that will be stored is staggering. Last Congress, I introduced the Consumer Online Privacy Act alongside my colleagues, Schatz, Klobuchar, and Markey, that would have established a new privacy bureau at the FTC to serve as a consumer privacy watchdog. And I'm pleased that the Budget Reconciliation Act that we're now considering in both the House and the Senate, has a call for action here by giving a billion dollars to the FTC to establish this bureau over 10 years to hire the technologists and the data scientists needed to keep pace with these digital threats.

I know my Republican colleagues in the Safe Data Act also called for a similar amount of money to be spent by the FTC for privacy and data security. And as such, companies like Microsoft and others have called for greater investments, today's witnesses, I know, will also underscore this need. Two of our witnesses, Professor David Vladeck and Ms. Maureen Ohlhausen, have served in senior positions at the FTC and have been on the front lines of enforcement actions against companies that misused or neglected their security of personal data.

We value their insights in how harm can be done, and that tools and resources are needed at the FTC to hold companies accountable. Mr. Vladeck, in your written testimony, you said the new Privacy Investment Bureau could be a real game changer. Mr. Soltani, who's going to be joining us virtually, was one of the first technology experts hired by the FTC, and I know he's been sounding the alarm for years about the need to get the right resources. More technologists so the FTC can deliver more. So I look forward to asking him questions about that.

And Mr. Reed, I was pleased to read your testimony, that you have a strong statement in support of first time civil penalty enforcements for the FTC in cases of privacy violations. So thank you all for being here. Thank you for all the work all of you have done on this important issue. And now I will turn it over to my friend and colleague, Senator Wicker, the Ranking Member, for his opening statement.

Witness Testimonies

[AUDIO] [VIDEO]

Cantwell: We'll now turn to our witnesses. Mr. David Vladeck, professor and Faculty Director of the Center of Privacy and Technology at Georgetown Law and former director of the Federal Trade Commission, and Bureau of Consumer Protection. Welcome. Ms. Maureen Ohlhausen, Partner and Section Chair, Baker Bots, former acting Chairman of the Federal Trade Commission. Mr. Ashkan Soltani, who's joining us remotely, an independent researcher and technologists, but former Chief Technologist for the Federal Trade Commission, and Mr. Morgan Reed, President of the App Association of Washington, DC. So welcome to all of you. And we'll start with you, Professor Vladeck.

Vladeck: Well, good morning, Chair Cantwell and Ranking Member Wicker. And I was going to say other members of the committee, I'm sure they file in. I'm David Vladeck, I'm a law professor at Georgetown Law School. And as the Chair mentioned, I'm the former Director of the Bureau of Consumer Protection at the Federal Trade Commission.

I strongly support the legislation before Congress today. It would provide funding to the FTC to create a new Technology Center Bureau to safeguard your constituents' privacy and data security. This proposal builds on the Chair's 2019 privacy bill, which also calls for a new technology bureau within the FTC.

I support the legislation because it will begin to rectify the chronic underfunding and understaffing of the Federal Trade Commission. It started in 1980s, when the FTC's budget and staff allocations were literally cut in half. Since then, as both of you have mentioned, the nation's gross domestic product has grown exponentially, and the FTC now enforces more than 50 additional laws than it did back in 1980.

But today, the FTC is significantly smaller, both in terms of staffing and funding than it was in 1980. As best as I can tell, that is not true for any other federal agency. And because federal budgets are based on prior year appropriations, the FTC is still lagging far behind its sister agencies, including among others, the SEC, the CFPB, and the FCC. But unlike other agencies, the FTC pays for itself. The FTC almost invariably, year after year, returns more money to the Federal Treasury than it gets. Why, because FTC civil penalties, including, for example, the $5 billion penalty the FTC imposed on Facebook, goes straight to the Treasury. $5 billion would pay for more than 15 years of the FTC's budget. If the FTC were a company, we'd all want to buy stock in it, because it always generates more income than it spends.

I urge you to pass this legislation to give the FTC the tools that it needs, desperately needs, to fend off and punish privacy violations and other digital harms. From internet scams and data breaches, to dark pattern manipulation and ransom square attacks. Without more resources, especially more technologists and engineers, the FTC will simply not be able to stem the growing tide of attacks on privacy and other digital harms. As a result, the cost to the United States will continue to vastly exceed the sums proposed in this legislation. Not enacting this bill would be penny wise and pound foolish. I know that some on this committee think that funding and the creation of a new bureau should await federal privacy legislation. I respectfully disagree. Your constituents are at risk today, and that risk grows as privacy averse business models grow.

Just read the Washington Post today about all of the internet enabled tools in one's household that are all collecting enormous amounts of sensitive information over which your constituents have little control. Both of both of you talked about data breach. Well, identity theft is essentially predictable debris of an internet economy that doesn't really care about data security. We still are plagued with data breaches. So the FTC is really the only privacy cop on the beat. It's time that Congress gave it the tools it really needs to be in this fight. So thank you so much for inviting us here today. I'm happy to answer any questions.

Cantwell: Thank you Professor Vladeck. Ms. Ohlhausen, thank you for being here.

Ohlhausen: Thank you. Thank you, Chairman Cantwell and Ranking Member Wicker and the other distinguished members of this committee for the opportunity to testify at this important hearing examining how to protect consumer privacy. As you've already noted, I'm Maureen Ohlhausen, I'm a partner at the law firm of Baker Botts, and I also had the pleasure of serving as an acting Chairman and Commissioner at the Federal Trade Commission, our nation's leading consumer protection agency.

As the collection use and sharing of personal data has continued to grow, the FTC is reaching the limits of its current tools, and consumers and businesses are increasingly required to navigate a tangle of confusing and often inconsistent privacy requirements from various levels of government. And to safeguard consumer privacy in today's environment, Congress needs to enact a comprehensive national privacy law. And that's why it's paramount that members of this committee returned to the bipartisan negotiations conducted in the previous Congress.

A new law should have several components. First, legislation should provide consumers clarity and visibility into companies data collection use, and sharing practices, as well as choices regarding these practices calibrated to the sensitivity of that data. Second, legislation should provide a national and uniform set of protections and consumer rights throughout our digital economy. Third, it should ensure strong enforcement that protects consumers from harmful data practices, while allowing companies to provide innovative products and services that consumers want. And while some have raised the possibility of the FTC undertaking a privacy rulemaking under its current general, unfair and deceptive authority, I'm concerned that a potential FTC privacy rulemaking may actually distract from focusing on achieving these key objectives through legislation.

And there are several potential problems with an FTC rulemaking. First, the scope of an FTC rulemaking under the agency's current UDAP authority is much more limited than what Congress can achieve statutorily. For example, the requirement of access and correction rights for consumers, which we've seen in a number of proposed bills, is likely not supportable under the FTC's current general authority. And some of my fellow panelists have acknowledged the limitations of the FTC's current authority and their testimony. Second, an FTC rulemaking may not preempt state laws and regulations, even conflicting state requirements. Thus, an FTC rulemaking could simply produce the 51st set of privacy requirements, rather than a single national framework that applies no matter where consumers live, work, shop, or visit. And this would lead to even more consumer and business confusion and a fragmenting of consumer rights. And it would also be particularly burdensome on smaller firms that lack the resources to deal with such regulatory complexity. Third, Congress puts significant limitations in place for FTC UDAP rulemaking, absent specific guidance to the contrary. And where Congress has enacted specific privacy laws, such as in the areas of children's privacy and credit reporting, it is given the FTC notice and comment APA rulemaking authority to implement clear statutory direction. Absent such clear statutory guidance and streamlined rulemaking authority, the FTC

must proceed under the more deliberate Magnuson-Moss process, which will slow the implementation of consumer protections that are widely supported by Congress.

Now there's no question that strong privacy law needs to include strong FTC authority to protect consumers' rights. A single federal privacy law that gives the FTC more enforcement authority will dramatically strengthen consumer protections. And it should authorize the FTC to find companies for certain first time violations, and, in certain cases, to issue rules to keep up with developments in technology. It should also give the FTC more resources. State AGs should be given the power to enforce any new federal law. And a consumer privacy law, though, should not include private rights of action with punitive or statutory damages that would primarily benefit lawyers and result in class actions that provide little if any relief to actual victims.

Giving the FTC specific authority to provide consumer redress would be an effective way to enable consumers to be compensated directly and promptly when companies engage in harmful data practices. So thank you again for the opportunity to testify today. And I look forward to working with the committee and all stakeholders to craft strong national privacy legislation.

Cantwell: Thank you very much, Ms. Ohlhausen. Now we're going to hear remotely from Mr. Ashkan Soltani, independent researcher and technologist, and Former Chief of the Federal Trade Commission.

Soltani: Hello there, can you hear me all right? Perfect. Chair Cantwell, Ranking Member, Wicker, and members of this committee. Thank you for inviting me to appear here today. My name is Ashkan Soltani, I'm a researcher and technologist, formerly Chief Technologist at the FTC. Since departing FTC, I've helped support state level privacy and tech enforcement, both as an expert and through my involvement through Georgetown Law where I'm a Distinguished Fellow at the Institute of Law and Policy and at the Center of Privacy and Technology.

I also helped author California's landmark privacy laws, the CCPA and the CPRA, Prop. 24, which California voters enthusiastically passed last year. I've seen firsthand the challenges in crafting and enforcement enforcing laws that constrain bad behavior in the current digital ecosystem. I'm pleased to be invited as Congress in this committee are considering significant changes to the structure and funding of the FTC. The proposal to create a fund and new bureau at the FTC is a strong step forward at providing the commission with new resources it needs desperately 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 placing unfair and deceptive trade practices related to privacy, data security, identity theft, and data abuses.

I've submitted my written testimony for the record, but I'd like to highlight three key points, which I hope will inform the discussion today. One is that the FTC is critically under-resourced to oversee the nation's myriad of privacy and cybersecurity issues. With a bare bones staff of about 40 attorneys and a handful of technologists, their resources pale in contrast to their counterparts in other countries. The German DPA, for example has 745 staff and nearly 100

tech experts enforcing their law for a country one quarter of the population in the U.S. Similarly, France, which has one-fifth our population and employs nearly 200 staff, including 30 tech experts. The resource problem is exasperated when businesses choose to litigate a case rather than accept a settlement.

By some accounts, litigation can occupy one third to one half the commission's entire privacy division on a simple matter. That's half of the entire federal privacy staff working on one case for years at the exclusion of other critical work. Similarly, the FTC's Bureau of Enforcement is tasked with overseeing compliance with all of the hundreds of FTC's consent decrees. In addition to a myriad of obscure laws relating to, for example, made in the U.S. stay in textile label. The same lawyers who ensure that social media companies have robust privacy and data security programs are also making sure the labels on bed linens are correct. In fact, many of the big tech companies, which this Congress is presently concerned with, such as Facebook, Apple, Google, and others are already under consent decree with the commission, but the FTC has limited resources to adequately monitor that these firms are complying with the terms of their order. One former FTC enforcement staff has publicly stated that the FTC rarely even reads third party assessments provided to it.

Additionally, the FTC doesn't need just more resources, it needs the right resources. Technology and data pervades nearly every aspect of today's online marketplace. Data security, data abuse, identity theft all have one thing in common, technology and the underlying data that they rely on. Narrowly constraining the new bureau to solve only one of those problems, privacy would fall short of the consumer protection goals laid out by FTC and this Congress.

I suggest instead, Congress support the creation of the Bureau of Technology and Data Protection. This may seem like a small point, but names do matter. As I said before, most of the harms don't concern just privacy, but data, and data abuse. I have long advocated for the creation of a new Bureau of Technology with a mission and expertise to investigate harmful practices across the technology ecosystem. This may be able to provide a hub of resources that would serve across the agencies, many consumer protection missions, incentivize collaborations, and encourage efficiency, similar to how the EPA functions cross division.

Alongside the funding, Congress should take steps to ensure that the Commission hires a wide range of staff to this bureau, outside of just traditional lawyers, economists and even technologists like myself. Importantly, the agency should hire statisticians, UX designers, social scientists, and behavioral researchers, such as experts in child development. We can guide the complex cases that come before them across a myriad of technology issues such as dark patterns, manipulative design, and algorithmic discrimination.

Finally, in additional to more resources, I support my panelists' call that the FTC needs additional legal authority to meet the challenges of the digital economy. While expanding the commission's budget is a great first step, this Congress should complement that funding with additional privacy authority so that the agents can fulfill its mission.

This is why it's critical that this Congress pass federal privacy legislation that builds upon, but does not preempt privacy legislation adopted in states like California and Colorado. I'm happy to go into what attributes of such legislation should look like but based on my experience in California, but most clearly is the ability to allow experimentation in the states as we seek to find the appropriate approach to the complexities of the digital ecosystem. Thank you for the opportunity to testify today. I'm excited to work with you all on helping to solve these challenges.

Cantwell: Thank you. Thank you very much. We'll now hear from Mr. Morgan Reed from the App Association who is here in person. Thank you.

Reed: Chairman Cantwell, Ranking Member Wicker, my name is Morgan Reed, and I'm the president of The App Association. We're a leading trade group representing small software and device companies in the app economy, a $1.7 trillion global sector that supports roughly 5.9 million jobs here in the U.S.

I'm here to share the perspectives of App Association members, many of which are in your states, on the need for strong federal privacy laws and enforcement. And when I say in your state, I'm not doing some kind of hand waving blanket gesture. I'm talking about real companies. Chair Cantwell, in Spokane we have Mighty Call, which provides a cloud based communications platform for small businesses to connect teams remotely. In Starkville, we've got Buzz Ambassador, they provide a management platform for brands to use ambassadors promoting a product across social media. And in my written testimony, there are examples for every single one of your states, and in every single one of the districts in this country.

We change the way we're doing business today, whether it's farming, education, communication, and sometimes just having fun. These companies rely on consumer trust much more than large companies with brand recognition, and privacy is the leading factor. According to Pew, 63% of consumers say they've deleted an app due to privacy concerns, and 65% cite trust in brand as their number one consideration when deciding whether to allow access to their information. My member companies are small and can't buy a Superbowl ad to create brand awareness. So when we try to reach customers through the app stores, we rely heavily on the trustworthiness of the ecosystem, and the marketplaces within. The Federal Trade Commission and this committee plays an important role in maintaining that trust by maximizing consumer protection, while fostering growth in the economy.

To better protect consumer privacy, we urge you to take these four considerations into account. Number one, Congress should set the scope and purposes of the FTC enforcement authority and resources on privacy. The existing regulatory framework for the FTC does not have the tools to deal with the more complex data and privacy questions that arise. The rest of the world has surged ahead of the US on these questions. When Europe instituted the GDPR, it was clear the US would have to act if just to harmonize, but now 16 other countries have national privacy laws matching GDPR. And as Ranking Member Wicker noted, there's 100 more countries with some form of national privacy law, and the US still has nothing. The FTC needs better privacy tools based on the risks data processing activities pose to consumers and the

expectations that people have about its use. It's up to Congress to set forth the overarching purposes and specify the limits on FTC rules. Failure to act hurts American citizens and American competitiveness globally.

Number two, if Congress doesn't act, we've seen how the FTC is forced to stretch their authority. The FTC is recent effort to use breach notification to cover unauthorized sharing is an example how the FTC has to cobble together a solution in the absence of congressional action. Just like Tom Hank's character in the movie 'Castaway', using ice skates to open coconuts, the commission is settling for the tools it can find, rather than the right tool when it proposes to enforce a breach notification rule is a privacy law. But we are not on a desert island. Congress can and should make the right tools for the job.

Number three, Congress should produce one national privacy framework. The single most important policy decision Congress can make to combat existing and future privacy harms is to enact comprehensive privacy legislation that grants strong consumer rights to the citizens of all 50 states simultaneously. A patchwork will make it hard for small businesses like mine, and comparatively easy for big companies with 100 lawyer compliance departments. In short, preemption is essential to the success for the little company.

And number four, Congress should avoid antitrust measures that prohibit some of the most important platform level privacy controls consumers and app makers rely on today. Big companies doing business on the app stores, Epic Games and Spotify and others, have their own big brand, and some of them don't want the app stores to manage the platform. However, we urge you not to undermine trust in the app economy with bills that would prevent key privacy protections my members rely on to bring consumers to market. To be clear, we're not opposed to, and in fact support, the FTC vigorously enforcing the law on privacy and on unfair methods of competition.

For example, on the competition side, the Commission has the opportunity to clarify the applicability of its UEMC authority to standards essential patents. Anti-competitive [inaudible] abuse harms consumers and small businesses and competition alike. And this is an example of where the FTC guidance can help. But ultimately, the economic health, education, and frankly, opportunities for growing new businesses created in our country depend on a robust and appropriately funded FTC.

Congress needs to get this right. And they need to do it now. And without it, we're left with giving the FTC a pile of money and they're going to end up spending it on additional ice skates to open coconuts rather than the tools that they need to solve the problems that we face today. Thank you.

Question + Response

[AUDIO] [VIDEO]

Cantwell: Thank you to all the witnesses. I know there's a vote that started so I'm going to ask my questions and then have Senator Wicker and Senator Baldwin ask theirs and I'm going to run and vote and then we'll be back and hopefully our colleagues who were over voting now will join us.

I heard what everybody said to their testimony. So, but also just so we have clarity, do each of you support more resources at the FTC, similar to what we've been talking about as it relates to this reconciliation item on the FTC having more of a privacy enforcement authority? Professor Vladeck?

Vladeck: Yes.

Ohlhausen: Yes, the FTC needs more resources.

Reed: Yes, the FTC needs more resources.

Cantwell: Mr. Soltani. Mr. Soltani? I'm pretty sure. Do you support more resources? Like a privacy bureau at the FTC?

Soltani: Correct.

Cantwell: Okay. So the question seems to be, and actually Ms. Ohlhausen, I heard you also say you are also first time civil penalties.

Ohlhausen: Yes.

Cantwell: So everybody, I think also agrees on that. Is that right? Everybody agrees on first time civil penalties?

Vladeck: Yes.

Cantwell: Mr. Reed?

Reed: Yes. As part of a federal privacy law, I think that it's worthwhile to make that available.

Cantwell: Okay. So the issue is that right now, we have a volume of cases. And we have a technology gap. And we don't have people to do compliance. What do we need to focus on when we say to the FTC, here's the resources. We definitely want to talk about a new privacy law. But what do we need to focus on to make sure that the resources at the FTC really focus on these issues?

When Mr. Soltani mentioned, I mean my impression is we basically have been using current tools to enforce basically deception in current privacy practices, and then having fines for

failure. But as Mr. Soltani says, the compliance of that, post that, seems to be greatly lacking. So Mr. Vladeck, what does this agency need to do to focus this?

Vladeck: Well, as I said in my written testimony, the FTC needs resources. One area in which we need resources is being able to hire more technologists and engineers. I don't think the FTC has ever had a cohort as many as 10 technologists on staff, Ashkan was the second technologist we hired, and that was in 2009. So there's really no end to the need by the FTC for resources.

But when it comes to enforcement, oversight of existing consent decrees, there is a division within the Bureau of Consumer Protection that has about 45 staff members, and oversees more than 1,000 ongoing consent orders, or litigated orders imposed by a court. And just the volume of orders that need to be sort of reviewed and subject to reporting requirements, overwhelms the ability of staff to do the kind of surveillance of a company under orders is required.

And so this is one area where, you know, resources are desperately needed because, you know, take a look at Facebook, it was the one of the first real major privacy orders we engaged in. We did not have technologists and staff who could spend time reviewing closely what the company was doing. And that's an endemic problem. And it's going to be an enduring problem unless Congress devotes more resources to the FTC. I was a triage nurse for four years, really, that was what I did. I tried to reallocate resources to the most dire function that the FTC could…

Cantwell: Well, I want to ask Mr. Soltani about this, because I worry that people are paying the fines and then going back to practices knowing that we don't have time for compliance. And this is everywhere in the federal government. Senator Wicker and I had to work very hard on aviation reform, which was the same issue of what did the FAA have as far as technologists to really understand the technology that they were reviewing.

So we need an upgrade across the federal government, but clearly if we want compliance on safety, we do. Mr. Soltani, since you mentioned a broad group of people, but don't we just need basic people who understand software operations and technology?

Soltani: It depends on the scope of the order. But absolutely, I think having expertise in, for example, the matters under order. So Facebook has a compliance program that they rely on a third party assessor for. And in some cases, the FTC doesn't even automatically receive those, they have to request those assessments. But then, as David mentioned, you need not only resources, but the right resources that can actually attest to whether these assessments are accurate, are done in the right scope, or even whether the assessor has the skills necessary. A lot of them are just checklists. So I think we need expertise, for example, on data security API's assessments in those groups overseeing the orders, compliance with the orders.

Cantwell: Yep, I would. I'd like to see a more formal list from somebody, but we'll keep moving on the process and then see.

Vladeck: Can I add just one quick thing, you know, in most privacy cases, there is no fine or nothing in terms of redress for the first violation. There is no original finding authority and because privacy harms, you know, are not monetary, the first violation is basically sort of, you know, consequence free other than the…

Cantwell: I will get to you Mr. Reed, but I will let Senator Wicker go ahead and then I will get back to you when we come back. And then Senator Baldwin.