FEDERAL TRADE COMMISSION

NIXING THE FIX

A WORKSHOP ON REPAIR INSTRUCTIONS

Tuesday, July 16, 2019

12:30 p.m.

Federal Trade Commission

Constitution Center

400 7th St SW

Washington, DC 20024

FEDERAL TRADE COMMISSION

I N D E X

P R O C E E D I N G S

MS. DAFFAN: Good afternoon, everyone. Hello, my name is Kati Daffan. I'm with the Division of Marketing Practices here at the FTC, and it's an absolute pleasure to welcome you all to today's event. Before we get started, I have the absolute pleasure of reviewing some required administrative details with all of you.

Please silence any mobile phones and other electronic devices. If you need to use them during the workshop, please be respectful of the speakers and your fellow audience members. Please be aware that if you leave the Constitution Center building for any reason during the workshop, you'll need to go back through security screening again. So especially if you're participating in a panel, please bear that in mind.

Most of you received a lanyard with a plastic FTC event security badge. We reuse these for multiple events. So when you leave for the day, please return your badge to security on your way out. If an emergency occurs that requires you to leave the conference center but remain in the building, follow the instructions provided over the PA system. And if an emergency occurs that requires the evacuation of

the building, an alarm will sound, and everyone should leave the building in an orderly manner through the main 7th Street exit.

After leaving the building, we'll all turn left and proceed down 7th Street and across E Street where there's an FTC emergency assembly area and remain there until instructed to return to the building.

If you notice any suspicious activity, please alert building security.

Please be advised that this event may be photographed, webcast, or recorded. By participating in this event, you are agreeing that your image and anything you say or submit may be posted indefinitely at FTC.gov or on one of the Commission's publicly available social media sites. And please -- I see that you're all doing this -- take seats rather than standing up for fire code reasons.

Restrooms are located across the hallway just outside the conference room. Almost done. The cafeteria will be open until 2:00 p.m. and then will offer limited service until 3:00. So please note that it will be closed during the break.

And then here's the last thing on this level, tune into it. There are question cards that

are available in the hallway and on the information table immediately outside the conference room and there are also FTC staff throughout the room who have question cards. If you have a question, raise your hand, get a card, fill it out, and FTC staff will come and get it.

For those of you participating by webcast, you can tweet your questions at @FTC using the hashtag #nixthefixftc. Please understand that we may not be able to get to all of the questions today, though we'll do our best.

Now, I'm honored to introduce Commissioner Christine S. Wilson, who will provide opening remarks. You should look at her entire bio in your program. You'll see an exceptionally broad array of experiences that all inform her work as a commissioner here.

She's practiced competition and consumer protection law at law firms such as O'Melveny & Myers and Kirkland & Ellis and also as in-house counsel, including as senior vice president at Delta Airlines. She also spent time in the FTC's Bureau of Competition and as chief of staff for then Chairman of the FTC Tim Muris.

Please join me in welcoming Commissioner Wilson to the podium.

WELCOME AND OPENING REMARKS

COMMISSIONER WILSON: So you can look very closely at my bio and one thing that you will not see on there is any ability to fix or repair things. I definitely trust the experts on that.

So let me start, first of all, by welcoming you to the FTC's Nix the Fix Workshop, and then, second, with a question. How many of you watched "MacGyver," not in reruns, not the second one, but the original in the '80s. Did anyone watch? All right, nice.

So as I was preparing for this, I had the opportunity to go back and watch some of the snippets and videos and some of the cooler tricks that MacGyver has done. My favorite was when he was stranded on top of a mountain with a pilot from a downed aircraft. And there were enemy soldiers coming up and they had to figure out how to get off the mountain safely. So MacGyver took a flare gun from the downed aircraft, and he pounded it with a rock while the pilot is screaming at him, what are you doing?

And so he narrowed the nozzle, and then he grabs the pilot in a bear hug. And he shoots the flare gun, which, of course, acts like a rocket thruster and carries them off the mountain to a safe

distance where he can open the parachute that he conveniently grabbed from the airplane and they drift to safety.

So, you know, I can't fix anything. I'm inspired by MacGyver and other people who can. And if you've watched "MacGyver," and it seems like a lot of you have, then you know one of the things that he says is there always seems to be a way to fix things. And he uses gum and chocolate and cold capsules and duct tape and whatever else he has in his pocket or in the immediate vicinity to fix things.

But in today's connected world, MacGyver may have had a bit more difficulty getting out of sticky situations. Today's consumer devices are more complicated than ever. And this may be blasphemy to the "MacGyver" fans out there, but I'm not sure that he could fix a smashed smartphone with gum and a paperclip. After all, he's not a licensed repair professional.

So we go to the heart of today's discussion. When should independent companies and consumers be allowed to repair consumer devices? A bedrock principle in a free market economy is that robust competition provides the greatest benefits to consumers. Competition incentivizes companies to

offer the best services at the most attractive prices. And it's based on this understanding that Congress passed the Magnuson-Moss Warranty Act in 1975.

The Warranty Act prohibits companies from linking warranty coverage to the use of particular products and repair services unless the company provides those products or services for free. The law was intended to protect consumer's choice and stimulate competition among small businesses vying to serve consumers' repair needs.

The FTC takes seriously our mandate to enforce the Warranty Act. Last year, the FTC sent warning letters to several companies whose warranties appeared to violate the anti-tying provisions of the law. Notably, recipients of those letters responded by adjusting their business practices.

Of course, while competition is beneficial, it's not the only laudable or worthy goal. Safety, privacy, data security, and other legitimate goals do exist. And manufacturers have explained that they impose limitations on who can fix consumer products, because of safety and security concerns, as well as product characteristics that consumers demand.

So today, replacing a battery is no longer as simple as popping in two new AA Duracells, or if

you're MacGyver, using a lemon and nails and a copper penny. Instead, this task can require application of specific adhesives that maximize runtime without causing a phone to overheat. Yesterday, I read an article about an iPhone that sparked and burned holes in a child's bedding, and facts are developing.

Of course, another concern is consumer privacy. A phone repair person usually is given a consumer's password, which comes, of course, with access to emails, texts, pictures, and other personal information or security programs that are stored on the device.

The battery replacement example illustrates how complicated repair questions have become. And weighing questions of competition and other goals, like consumer safety, can bring complexities. But challenging issues like these play to one of the FTC's strengths and, indeed, it's one of the reasons that I love being at this agency.

The FTC perennially pursues learning to inform its policy and enforcement approaches. We conduct R&D by engaging with industry participants, soliciting public input, and conducting or soliciting research. And as today's event indicates, we also hold hearings, workshops, and roundtables.

I anticipate that input from today's workshop will contribute to the agency's ability to assess the dynamics of the repair market in measured and thoughtful ways. Today's first two panels will explore limitations imposed by manufacturers on the availability of diagnostic tools, software, and replacement parts for products, the rationales for those limitations proffered by manufacturers, and the impact that those limitations have on the ability of consumers and independent repair shops to repair some products.

We will also consider the privacy, data security, and safety ramifications of allowing consumers and independent repair shops to make repairs. Panelists will endeavor to identify what costs are imposed on consumers and small businesses by repair restrictions and answer whether the costs and burdens are justified by other legitimate goals.

The third panel of this workshop will discuss whether a fix is needed or if competition is effectively protecting consumer interests and wallets. Panelists will explore the existing and currently proposed fixes. They will also discuss whether there are opportunities for consumers and independent repair shops to access the tools and information necessary to

make repairs without compromising data security, privacy, safety, and other legitimate goals.

So before we get to the first panel, I'd like to thank everyone who made this event possible. First, obviously, many thanks to the panelists and all of those who've already submitted research and comments in advance of this workshop. Second, thanks to Dan Salsburg from the Office of Technology Research and Investigation, and Christine Todaro and Claire Wack, from the Division of Marketing Practices, for planning this event. Thanks to our colleagues from the Office of Policy and Planning, the Division of Consumer and Business Education, and the Office of Public Affairs, who have all provided vital input.

And I'd especially like to thank my friend Bruce Jennings and Crystal Peters and their entire team for helping make your Wifi during this event possible. And, finally, I'd like to convey the FTC's appreciation to our in-person attendees, as well as those watching online via our live webcast.

Stakeholder input helps us advance our thinking on complex issues like the ones that will be discussed today. We anticipate and hope that this workshop will spark further conversation, research, and collaboration by and among industry, consumer

groups, researchers, and staff. We encourage you to submit comments and empirical research through September 16th of this year.

And now I'll turn it over to Claire Wack, who will be moderating the first panel.

PANEL 1: HOW DO REPAIR RESTRICTIONS AFFECT CONSUMERS AND SMALL BUSINESSES

MS. WACK: Good afternoon, and as Commissioner Wilson said, welcome to the Nixing the Fix Workshop. My name is Claire Wack. I'm an attorney in the FTC's Bureau of Consumer Protection Division of Marketing Practices. We will be hearing from our panelists on what impacts, positive or negative, repair restrictions have on small businesses and consumers. We will also discuss the potential safety concerns surrounding uncertified product parts.

Joining me in this discussion are Jennifer Larson, the CEO of Vibrant Technologies in Eden Prairie, Minnesota; Theresa McDonough, the owner of Tech Medic in Middlebury, Vermont; George Borlase, research staff member at the Institute for Defense Analysis Science and Technology Policy Institute and formerly of the US Consumer Product Safety Commission, where he most recently served as an assistant executive director for hazard identification and reduction; Nathan Proctor, the director of the Campaign for the Right to Repair at US PIRG; and Walter Alcorn, vice president of environmental affairs and industry sustainability at The Consumer Technology Association.

I'll be giving each panelist about seven minutes to offer their perspective, at which point we'll move on to a discussion. I will be accepting questions and will ask them as time and conversation allows. If you have a question, please write it on one of the question cards and FTC staff will bring it up to me.

With that, we will hear first from Jennifer Larson of Vibrant Technologies.

MS. LARSON: Thank you, Claire and Dan, for making this possible. I appreciate the opportunity.

So a little bit about myself, I'm the owner and CEO of Vibrant Technologies. I've run the company for 20 years, which means I was a toddler when I started it. We're primarily a reseller of refurbished servers, storage networking, and we're a small company.

I also wanted to remark, because I'll touch on this in a little bit, I'm also the founder and CEO of an autism center. My son has autism; he turned 19 today.

And I also want to make the point that I'm not a PowerPoint whiz. Please don't get your hopes up that in any way this is going to be that amazing.

So I was asked to come and talk about, from

my perspective, how these policy changes over the last 20 years have affected my business and my customers. And I can tell you, over the past 20 years, the OEMs have become increasingly hostile to my market and third-party maintainers. They're doing everything in any way they can to try to stop and control the lifecycle of the equipment.

A lot of times we don't have the ability to repair and it goes straight to a landfill. And a lot of times the resale of the equipment, now, sometimes we can't even sell it at all. So things have changed a lot in 20 years.

Our biggest issues at Vibrant are licensing and tying. Because I'm a B2B and we do server storage and networking, I deal less with consumers. So these are all licensing issues, property rights issues, as well as tying -- when you tie one product, like Christine was saying, to the next. We see that all the time.

I'm going to actually go over a few examples that are just right off my floor. Right before this, when Claire said we needed slides, I went to the back and I just said, okay, guys, download on me, what did we run into today? So I'm going to give some examples. I'm trying to keep them high level, even

though they sound technical, because I want you to see real life, how this stuff affects a business.

So here's an example -- these are from July 1st. So we sold a machine that was $40,000, an IBM machine, to one of our customers who's a broker in Denmark. They then sold it to a client, an end-user client. Well, apparently, when they got it there, the firmware level was too low to connect with the other equipment that they have in their data center. So they would need what's called a firmware upgrade.

Firmware, for those who don't know, makes your equipment connect. So it's interoperability. It's like when you have a printer that you buy to connect to your laptop at home. If every time you got a new laptop or device, you had to buy a new printer, that's what this is kind of like.

So they couldn't use it. They had to ship it back. And, you know, we'll probably end up with -- with servers, what we're seeing is because of these issues we end up parting them down and reselling the parts to maintenance companies because it's becoming almost impossible to sell servers because of this type of situation. And it's even worse in the US.

An example in the US would be, say we're going to sell a machine to a customer in the US and

they want it quickly. That's often a benefit of used equipment is we have it in the warehouse, right?

Well, so then they have to transfer the serial number and it will make it a lengthy three or four weeks. And then they have to -- they'll say, okay, if you want to get it under maintenance, that's going to be another however long. And in the end, they'll end up buying a new machine because IBM will say, well, why don't you just buy a new machine and we'll give you maintenance super cheap, way cheaper than you'll get on that used machine, and, you know, this can just go in a landfill then basically.

I don't know if that makes sense, if I'm going too fast on those topics. Oh, my gosh. I have to go quicker.

Okay. So product defects, another example is the POWER8 RAID controllers. They actually have a defect and you can only get the -- fix them if you get a support contract. So basically these are worth 1,200 bucks if they're fixed, but you have to buy the support contract, which is more than that, to sell them. So they just get scrapped.

Another example is upgrading memory. You can't even upgrade memory, even though it's better for power consumption, unless you have, again, the

firmware upgrades. So you have to buy the maintenance again, tying or suspected tying.

Or in my own environment, our Cisco ASA in my production environment had a bunch of fixes that needed to be done because of their software that made it vulnerable. So these are problems in their actual product. But I can't get those fixes unless I buy, again, a support contract.

And here's one from my autism center because with my own son and all the kids, they have to constantly buy new iPads because you can't update the iPad to have it high enough to get a lot of the programs that are useful for kids that are nonverbal or need an iPad for communication. So I mean, I could give you examples for hours. It's just everywhere and it's affected my business in a very major way.

Oh, I forgot I put this one up here. I wasn't sure. So the whole Magnuson Act, I had a furnace go out. We had two furnaces. It was 60 below in Minnesota.

Dave, you probably remember this, a few years ago.

I couldn't get it fixed because I wasn't on the emergency list because I had another furnace. So a friend of mine who lives down the road said, I'll

come over and fix it. I'm, like, yes, because it's freezing on that side of the house. And he did. Well, then the next time someone came out, the gentleman says, your warranty is going to be voided because I can tell there was a third-party repair.

I just about lost my mind. I said, it was 60 below and you guys couldn't get here. And I'm supposed to -- luckily, he was misinformed, because I about -- yeah. So that's my consumer experience.

So overall, I've lost millions in revenue for sure. I mean, I can't even quantify over 20 years how much I've lost. The whole business has substantially changed from whole servers, like I was saying, to having to part them down and sell to maintenance companies. So you get these huge chassis that are going in landfills.

Inventory overall has become less valuable. We have angry, angry, angry people when they find out that their hardware is basically worthless when they want to sell it back to us because we can't give them the kind of dollars they think they should be getting for it when they put all this money into it, and, you know, much more equipment going into landfills.

I did want to say one real quick thing that's not on here. So Cisco had a really fun thing

that came out recently. They're calling it the smart licensing. Instead of the license being perpetual on the device, now you have a subscription to the license and it has to call home every day. And if it doesn't call home to Cisco within 30 days for some reason, they'll shut down your equipment. Not only that, but you can't even sell it on the used market anymore. If you're going to sell the equipment, you have to sell it back to Cisco.

So that's just another fun point. And that's about it. Thank you.

(Applause.)

MS. WACK: We'll hear next from Theresa McDonough.

MS. MCDONOUGH: I'll just do my comments from the desk because I don't have a PowerPoint.

So today, I'm here to share my experiences as a repair technician. I own my own cell phone and computer repair shop in Middlebury, Vermont. Many of my customers are blue-collar workers, students, and farmers.

Over the years, I've come to realize just how reliant we all are on our phones and computers. Most of my customers will say, I can't even be without my phone for an hour. It's pretty funny because most

of the time it's the adults who have the problem and not the teenagers, despite what we may all think. For many of them, you know, people are running their small business on their device. So a day without a phone really could mean a day without being paid.

What I find most amazing is that many of my customers are return customers. If you have a family of four or five, as many of you may know, it's not unusual to see something being broken every other month. With the average device costing anywhere between $500 to $1,000, this could mean a replacement cost of up to $6,000 a year for the average family, if they could not repair their device. That's more than most people pay in property taxes. At my shop, I can often save these customers thousands of dollars, with most repairs only costing about $80.

I recently had a single mother in. She broke her cell phone and she had her own landscaping business. This woman was literally crying because she had to decide between paying her electric bill and fixing her phone. And even still, this cost of repair was going to be significantly less than replacing it, but it was still a really hard decision for her.

I've been fixing phones for about seven years, just out college. After that, I started my own

business. And I have seen the repair industry literally do a 360. Although some devices have gotten better, a lot of devices have gotten a lot worse to repair.

Just for example, what I see every day, like, a Samsung S4 used to be super easy to take apart. You could change the battery out. I'm sure most of you have had phones where you can replace your own battery.

I have a device here. This is the Samsung S6. This device is completely sealed. If I had a customer come in and their charging port was broken, I would have to tell them, in order to fix your charging port, I have to also fix your screen because they glued everything shut. And this is a common occurrence with many devices.

Apple's phones are fairly repairable; however, I've seen their computers go from upgradeable, where you could put in a new hard drive, a solid state, which makes them much more reliable and faster, but now you have their computers where everything's soldered right to the logic board. It's almost like looking at an iPad inside.

I had a gentleman recently who is a flight attendant and his iPad literally died two weeks after

the warranty was void. He had an iPad Pro, very expensive. And, unfortunately, I don't do micro-soldering. It is a very technical, labor-intensive sort of repair. And so this poor gentleman was stuck without a device he could use and he had just paid a lot of money for it.

I would say one of the hardest parts for me to source is good aftermarket lithium batteries. Batteries are consumable. It's not a matter of when, it's if, you know, they're going to go. Instead of making these batteries replaceable, many companies use strong adhesives to keep them in. This never used to be the case.

The iPhone 5 used to have a pull tab. So why did companies go from having a battery that was easily removable to now basically gluing them in? I don't think this is adding any sort of innovation. This hasn't really changed the devices in my perspective, and I work on these every day.

A lot of companies claim, well, the batteries, when you go to replace them -- it's probably the only time that I see the potential for injury for any consumer or repair shop. And this is an issue that companies have created themselves. If you don't want us being injured by repairing the

battery, which is going to go, then why glue them in? Why not have them easily removable like they used to be?

And then you have companies like AT&T and Verizon kind of perpetuating this issue. They work on commission. So at the end of the day, they're not telling customers, hey, go up the street and get this fixed. They want to sell you a new device. In the US, we throw away 400,000 smartphones every day, and a good majority of these devices are repairable.

So I was just talking to a good friend of mine, Robin, who many of you may know. He owns Good Point Recycling. And he was saying, one of the most concerning issues to him is the billions of dollars in potential loss for small businesses because of the possibility of losing the refurbishing market. If companies start using blockchain and RFID parts basically that are not interchangeable, we're going to lose a whole sector of small business.

Basically, iPhones have parts that are basically synched to the logic board. So if that part breaks, that is no longer repairable. This technology is not prevalent, but it is coming down the pipeline. And that is really concerning for a lot of small repair shops.

Whether you believe in global warming or not, the environmental impact of e-waste is undeniable. And technology is playing a larger role in all of our lives. I just saw on the news the other day that robots are now being used in certain cities to deliver packages. Soon, most of the devices in our homes are going to have complex logic boards, and it's essential that we have the ability to fix these devices.

My biggest concern is, what is technology going to cost us in 10 or 20 years from now on a yearly basis? And will the less fortunate among us be left behind because of the economic costs of repairing or replacing these devices? What standards are we going to hold these companies to for quality and repairability? I don't really know of a standard of how long each device is supposed to last. I think, at the very least, we could offer some sort of repairability score for each device and make this available to consumers when they're purchasing.

I can confidently say that all of my customers have no idea whether or not their devices are repairable. So many times I've heard, had I known I couldn't fix it, I would not have purchased it. My customers want to be able to repair to their devices.

They want to be as environmentally friendly as possible. And that's why I'm here today, to give them a voice.

We need to wake up and see what corporations are doing. You know, they know we're so reliant on these devices and, at the same time, they're making them less repairable and not any better quality. It's their interests they're serving not ours. So please let's work together to find a solution that can work to address these issues for today's generation.

Thank you.

(Applause.)

MS. WACK: Next is George Borlase.

MR. BORLASE: Good afternoon, everybody. I was born in New York City, and I'm a big basketball fan. So I was really excited to be here to talk about fixing the Knicks. But then I reread the email. And they didn't sign Kevin Durant anyway. So it probably made it a harder discussion when they didn't sign him.

But I do want to take a second and thank the FTC for putting on the workshop. That is a great idea for a Knicks workshop though. I mean, you pay that ticket price for Madison Square Garden, you should be able to see a quality team, right? No comment on the

local team.

But I do want to thank the FTC for putting on this workshop and tackling a terribly nuanced topic. It's really complicated. And I especially appreciate the FTC's call for empirical data. Coming from the Consumer Product Safety Commission where we spend a lot of effort collecting consumer injury data, I appreciate your call for the data.

Also, as an engineer, I am supremely overconfident in my own ability to repair anything. So I really appreciate your comments because I would be the exact customer who would come in and say, somebody tried to fix this first, so I need you to do it for me, please.

My background though is safety and risk management. And so my comments today are really going to be based on that lens of consumer product safety. And I'm just going to start by putting out really there a couple of principles regarding repair, as we're talking about this today.

I think, first, regardless of who is doing the repair, do no harm or do no additional harm. Something's broken so it needs repair. But you don't want a repair that can make the product less safe than it was, especially when it was broken.

The second principle I would put out there is any replacement parts or software should at least meet the same safety standards or the design requirements as the original part. Look, everything is in a complicated system nowadays. But what we're trying not to do is introduce any new hazards from fire, shock, mechanical, et cetera, with a part that doesn't meet the same requirements as the original. For all these parts, as complicated as they are, there is a design process that goes through in the development of them. Decisions are made on the design to try and balance safety and a number of other things. And what you're trying not to do when you're putting a replacement part in is really kind of create a more hazardous situation than you might have had before in the original.

I especially appreciate, Theresa, the comments on batteries. That is one area where you definitely see, one, a number of counterfeit batteries. Every device now is going to lithium-ion batteries. Apple TV used to have two AA batteries in the controller. Now, it's a rechargeable lithium-ion battery. People want more power and a smaller footprint for all their devices. It's going that way. But I appreciated your comments about batteries

because from a consumer product safety perspective, when we see fires, et cetera, a lot of them are battery-related and a lot of them do become related to either a replacement battery or a battery that may not have been certified along with the original.

With these two principles in mind, I just want to take a minute to highlight why, in my view, balancing consumer and product safety and the right to repair is getting more difficult. And I think the Commissioner kind of talked about it before. We are definitely in the fourth industrial age, often called the exponential age.

Consumer expectations of their products are increasing rapidly, as is the complexity of the products that we're seeing. Industries used to really be hardware industries. They would build dumb metal boxes, for lack of a better way to describe the old washers and dryers, right? But they're no longer that way.

Hardware companies are really becoming software companies. You see it in automotive; you see it in appliances. And a lot of that is due to the real price drop in everything from sensors to control systems to programmable circuit boards, all of which really lowers the cost barrier to putting things into

products.

I remember when fidget spinners came out a couple of years ago. Everybody remembers those. There were fidget spinners, and there was one that had a little speaker, a Bluetooth shield, and a tiny lithium-polymer battery so you could play music through this terrible little speaker in your fidget spinner. Now, why did they do that? It's kind of like climbing Everest. Because it was there, right? But the ability to, in a fidget spinner, put in a Bluetooth shield, a lithium polymer battery, and a circuit board for it was really something.

Now, admittedly, there wasn't room for the battery circuitry that would protect the battery from overheating when you charged it. So there were some shortcuts taken. But my point being that the miniaturization of all these sensors and really the drop in cost for all this has really reduced the barriers to putting a lot of these additional technologies into devices that never really had them before.

So what does that mean? I mean, that really means the design and the manufacture of all this stuff is more complicated. The companies are balancing the costs -- and I think this is what we're hearing up

here -- that companies are balancing the costs of the material availability, complexity, and even more, the sustainability. Although, clearly I think there's a lot more discussion to be had on sustainability and lifecycle management for this.

I did want to kind of put together maybe a proposition of a framework of questions. I usually like to do it that way. I like to ask questions and kind of run things through a framework of questions. But as we're looking at the difficulties in fixing anything -- you know, I was thinking about the right to repair. And I always go back to my favorite answer from my favorite lawyer which is, it depends. So in trying to answer the "it depends," as the answer to the question of who should repair what and when, I would say, here's three questions to really maybe create a rubric of asking who can repair what and when.

The first question is, what is it that's broken and how is it broken; in other words, the complexity of the product and what's the complexity of the repair for the product? I think Theresa probably could talk to some fixes being easier than others on the phones, as an example, or for the networking equipment, also. So that's the first question.

The second question is, with what? With what are you going to effect the repair? And this is where I go back to the certified parts and the fact -- you know, bringing those principles in. That you are looking for a product that isn't going to create a problem that wasn't there before. That's the second question.

And then the third question I would ask is, by who? I mentioned being an overconfident engineer. But when you say the public has the right, what is your mental model of who can fix this? You know, they have certified service technicians that go to school for six to eight weeks to kind of learn how to repair some of these things. Probably not going to be able to do it for everybody.

When you're looking at a member of the public to repair something, I would say, what is your mental model? You know, I always used to go back to, on the safety side, a grandmother in Kansas. Is that something they could fix? Is that something, right? Because that's the exact opposite of me. But you have to have a good mental model of who is trying to effect the repair and what really are their abilities and skills enabled to do it.

So I just put those three questions out

there as maybe a framework of questions to ask as you go through the right to repair. So with that, I just want to say thank you again for the opportunity to be on the panel. And thank you again to the FTC for putting this together today.

(Applause.)

MS. WACK: Next, we'll hear from Nathan Proctor.

MR. PROCTOR: Thank you Claire, FTC. I'm excited to be here.

My name is Nathan Proctor. I'm the national campaign director with the US Public Interest Research Group's Right to Repair Campaign. We're a consumer advocacy organization that tries to put the public first. And we are concerned with the consumer impacts of restrictions around repair.

You know, I love "Star Trek," and they literally have six different devices on the Enterprise to do what one smartphone does. They could not imagine technology that powerful or useful. And as Theresa said, Americans dispose of 416,000 smartphones every day. We buy $1,000 supercomputers -- unimaginable technology to even people 15 years ago -- and then we're, what, recycling them for commodity value. It's an absurd -- something is wrong here.

And the truth is it's bigger than just smartphones, right?

Our relationship with electronics is kind of changing direction. And I think that there are some serious things that if we don't address we're going to lose fundamentally the democratic sense of maintenance and ownership of technology in our lives.

So when I talk about repair restrictions, I'm going to talk about kind of three categories. So first would be devices that are not intended to be repaired. They were engineered without repair as a consideration whatsoever. That's a choice that manufacturers make. They should be upfront with that choice, but that just exists in the world. Two are warranty repairs and three are post-warranty repairs.

So just talking about warranty repairs, I think for most people there's issues around warranty repairs. So for example, inconvenience, people do not have access to timely repairs. If your LG fridge goes out and LG needs to send a service technician and they just don't have enough and you're two weeks without a fridge, two weeks is a long time to be without a fridge. You can try that if you want, see what that's like.

But, largely, these things get fixed in ways that's satisfactory to consumers. But one of the things that we found is these warranties are conditioned to the manufacturer being the only person allowed to touch the device. And this is something that the FTC took action on in April of last year when they sent warning letters to six companies.

And I did a survey of 50 appliance manufacturers where I read their warranties and then I called their customer service lines or went through the email or chat features they had on their customer service and asked them, if a repair was done to this device by an independent, even if it met or exceeded your own repair standards, would my warranty be voided? And at the end of that, I had five companies that would honor the warranty in spite of independent repair and 45 that would inform the customer that no, they would lose their warranty.

And I think that that's an issue, not only because Magnuson-Moss kind of speaks to that in a way that would not encourage it, but also it communicates something to the consumer. The consumer is told the manufacturer controls this device, you do not control this device. If you try to take any kind of control of the device, you make your own decisions about the

device, you've broken your relationship with the manufacturer and they don't owe you anything anymore. And I think that that scares people off.

And I don't know how many times -- you know, Theresa said, people come in and they don't want to get something fixed because they're worried about their relationship with the manufacturer, regardless of their rights as consumers.

I recently had somebody send me a photo from an AppleCare response where it said, we're denying your AppleCare service because there were unauthorized modifications to the device and that caused the problems that you have. Now, that's carefully worded. I'm sure lawyers are involved because they're probably allowed to deny service to somebody who had unauthorized modifications in such a way that damaged the phone. Like, it's not Apple's fault if I try to soup-up my phone and break it.

But the truth is, the person just had their screen fixed and then an independent technician opens the phone up, immediately finds the problem -- something that they deal with all the time -- fixes it, completely unrelated to the repaired screen. But if you're a consumer, all you know is if I take this somewhere else, Apple's not going to help me anymore.

And that's not okay. This is a problem that needs to be addressed.

And so -- oh, I have this little thing.

UNIDENTIFIED FEMALE: Yeah, push the green button.

MR. PROCTOR: Push the green button.

So why is it so hard to fix our stuff? And I'm glad that George brought up these parts. The spare parts we use should be to the exact specifications of the engineers. I agree. Please sell us OEM spare parts so that we can fix things to the exact specifications or give us the schematics so that we know exactly how the thing is intended to work.

No one is out here trying to repair things in such a way that violates the engineering standards that were made. We just want to do the right job and we don't want to have to enter in a monopoly environment to pay through the nose to get it done.

Some of the other restrictions that we see, you know, diagnostic software, firmware we talked about, proprietary. I want to click through a couple of things. So this is the market share for iPhones in 2017. You see that the last four iPhones, 60-something percent of the market. So actually the

crowdsourced information for how to fix an iPhone is pretty good. And, in fact, we have reason to believe that some of the crowdsourced resources are being used to train Apple's own technicians thanks to some leaked stuff.

But here's the next problem. These are the Android phones on the market. So imagine you're Theresa and someone brings in that tiny little green one, brings that to you and says, I need this fixed. You don't have the parts, you don't have the schematic, you don't have the diagnostic software. How are you going to figure out how to fix that phone in a way that's profitable for your small business? You're just going to tell the person, I don't have enough time to troubleshoot this for you, you know.

Here's another -- these are all the screw heads. This is a sampling of screw heads out there in the wild. You know, some of these make sense. I like torque bits, they're really effective. You know, I think Phillips are overused. But some of these are just essentially like -- just purely to be a barrier for repair. They're just silly.

This is Willie Cade standing in front of a John Deere tractor. John Deere tractors are notorious because they have these extensive software locks. If

something goes wrong on that device, you need the John Deere service advisor software to come and let you get it running again, even if the device is completely fixed.

And this photo was in an article in Crain's Chicago Business. They found that the profit margin for repair was five times higher than the sale of new equipment. And I think an easy explanation for that discrepancy would be the repair is monopolized, the sale is competitive. And I think repair should be competitive. And that's what I've got to say about that.

(Applause.)

MS. WACK: Our last presentation will be by Walter Alcorn.

MR. ALCORN: All right, thank you very much. I appreciate the opportunity to be here today and address this topic.

All right, good. So my name is Walter Alcorn. As mentioned earlier, I'm the vice president for environmental affairs and industry sustainability at the Consumer Technology Association. I'll just disclose right up front, my focus for the past two decades has been on electronics recycling issues for our industry. So I come at this with a little bit of

knowledge from that point of view. But some of the other interesting twists on this are relatively new that I've picked up just in the last year or two.

I want to point out, for those of you that are not aware of the Consumer Technology Association, we're probably best known for the Consumer Electronics Show, CES, which is -- occurs every January in Las Vegas. I know a number of you have been to CES. I've seen a number of you at CES and encourage you to attend it. It really is the place where people go and see new technologies and see what is coming to the market, a lot of which does not pan out. So that is us.

We also focus primarily on consumer technology. So my remarks today, and during the Q&A, will be focusing on consumer technology, consumer electronics, not on the B2B side.

So I would just point out -- it's interesting. This whole discussion, I think, underscores the evolution in the notion of ownership that we're seeing in the economy right now. It used to be before software was embedded in these devices, ownership was very cut and dried. You owned it or you didn't. But now with software, that has become a little bit more complicated.

And in another twist -- and I think this is true of a lot of the folks in this room -- now we have services. So the combination of hardware, of software, and services is an interesting mix. And I think it does put some of these topics or issues into the gray area.

So I'm going to be quickly going over five different items. Let me just underscore one of the things that George said in his opening in terms of repair -- and I would say, in this case, I'm talking about the manufacturer role -- "it depends."

So there are different products that have different histories, and I think we need to acknowledge that from the get-go. It's very hard to come at this issue and come up with a blanket ideology that really applies to all products in the industry. So I think it's important that we look at each one at a time.

For example, these days you can go into a gas station and buy a cable to basically attach your iPhone to the car. You paid $5 for that. I don't think anybody is expecting the manufacturer to provide diagnostics to the consumer so they can fix the cable. You're lucky if it works, but you know that going in. That's the very low end of the market.

It changes as you go up in the market. And, frankly, some of the biggest fights we've seen have been at the top of the market because that's where there's demand and that's where the market is. And I think it's important for us all just to acknowledge that.

Now something that really does affect the way manufacturers look at this issue is a concept called extended producer responsibility. Usually we hear that term in the context of the area that I know best, electronics recycling. But, in this case, it applies across different topics.

The basic idea is this: The day is long gone when manufacturers' responsibility stopped when they sold the product. These days, manufacturers still have responsibility. They're still expected to have responsibility long after their product has been transferred to somebody else.

So for example, somebody earlier mentioned battery safety -- and I know this is going to come up throughout the day in terms of having batteries be removed -- as an important thing. About three years ago, I was in the office of OSHA and, frankly, I heard OSHA staff complaining about the access that consumers and others have to lithium-ion batteries. There are

lots of issues, I would say, competing priorities, as was said in the opening, that I think we have to acknowledge.

On recycling, we do have 24 states now that mandate some form of responsibility for manufacturers to recycle old electronics. And now we're seeing, as well, cybersecurity privacy protection. And I'll get a little bit more into that.

The last bullet there points out that we are seeing -- and a lot of us have been involved in legislation at the state level. None of those bills have passed, but they're still definitely a point of discussion. In effect, what those bills do is -- or at least they have the potential to do -- is create a new point of manufacture, but without transferring the responsibility that manufacturers assume when they make a product.

So to get very specific to the FTC, the FTC has issued guidance for manufacturers that make it clear that they have a responsibility during the lifecycle -- during the use-phase of their product that could be jeopardized, in my view, depending on what kind of legislation or government mandate that might be enacted.

So I would just point to the second bullet

there, which is -- there's actually -- in this FTC document, the Internet of Things and in Start With Security, they make a point of telling manufacturers to be very careful about the service providers you hire, to make sure your service providers implement reasonable security measures. Well, if manufacturers are required to provide all the software and the ability to repair, to change products, well, that pretty much goes out the window. I'm not sure how you reconcile these. This, again, is a rather complicated area that I think needs to be explored more.

And then I would just point out, we do have benefits of existing authorized repair networks. One of the things we're doing at the Consumer Technology Association, we're putting together an online system for consumers to find authorized repair services for mobile devices. We're planning on rolling that out at the end of the year.

And as part of that process, we've been getting lists of authorized repair providers by different manufacturers. That list is now in the thousands of facilities. There is competition out there. It's also something we would like to see more authorized repair facilities come online in order to have a more robust system.

But setting that aside, we do have things that authorized repair does provide, including the training that's been mentioned, quality control. We actually have -- some of the FTC issues are addressed through authorized repair networks, background checks.

And I would also point out, if we go down this road and the Government, at one level or another, requires that this information be available so that anybody can do repairs, we're going to change things in the secondary market for used devices. Because, right now, when you acquire, say, a used iPhone or a used Samsung device, you generally expect that that phone has only been messed with by those manufacturers or somebody authorized by those manufacturers.

That's not true with cars, at least in my day. Typically, if you get a used car, you expect somebody to have gotten in there and repaired it or maybe there are aftermarket electronics in there. That would fundamentally change the view of used devices. So there are consequences that I think we should keep in mind.

And then just to run through these real quick, some of the issues that the FTC I know cares about are potentially at risk from some of the solutions that have been put out legislatively.

And you can read through some of those, particularly the idea of remote access. Basically, the ability for a manufacturer to control what happens to data generated from the use of a device, pretty much goes out the window if you open up the device as has been proposed.

So that's it. I've gone over my time, and I appreciate it. Thanks for the opportunity to speak today.

(Applause.)

MS. WACK: Thank you. My first question is for you, Theresa. As someone who makes a living fixing things, what kind of issues are you encountering when you're trying to repair devices? You mentioned a sealed phone. What other things are you encountering?

MS. MCDONOUGH: Definitely access to reliable parts. I would say one of our most popular repairs are iPhones. And it's funny because in the rest of the world Samsung and Android kind of rule. But here in the US, we really love our iPhones. And sourcing these parts can be frustrating. Luckily, I've been doing this long enough that I now have a really reliable aftermarket manufacturer that I get my parts from.

But when you're first starting, or any small businesses is first starting, you can get really, what I call, shoddy parts. And it's frustrating. You can usually get your money back from this manufacturer. But it's more frustrating for the customer because they kind of lose their confidence in you. They get a part on their phone and say their phone starts phantom typing and calls their mom at 2:00 in the morning. That's a real issue. These phones, if you don't have reliable parts, they can start doing funny things. And it's not necessarily something that the technician did. It could simply be just from not having access to good parts. So I would say that's probably one of my -- at first was one of my biggest hurdles.

Luckily, now, I really try to source -- when I'm doing computers, for example, I really try to source OEM parts from devices that are being recycled. So we pull them off of actual Apple computers that might have been damaged from something happening. So we try to recycle these parts.

But every single time a new device comes out, you know, you kind of panic and you think, okay, what are they going to do to us this time that we can't fix. I really think it's not doing our customers any service to not allow them to upgrade

even the hard drives in their computers. That's something that you've been able to do almost since the existence of personal computers. And now everything's soldered in.

So it's like when you go to the store, you have to make that decision of what you want then and there because there is no changing your mind. So that's probably the main thing.

MS. WACK: Thank you.

George, during your time at CPSC, the agency issued a letter stating that uncertified parts were more dangerous than those that were certified. Does that mean that the parts that manufacturers use are the only safe parts? Are only manufacturer parts certified? What can you elaborate on?

MR. BORLASE: Sure. I'll go general. What we were doing, when I was at CPSC then, was trying to address what I talked about in my points here, too, which was you're trying not to create a problem when there wasn't necessarily a problem before or something was being managed by the way that part was designed and by putting a different part in you create a problem. I mean, kind of like what Theresa was describing as a specific example.

So in terms of something that's certified

versus uncertified, I will say that we stopped short of saying it must bear a specific mark. But certainly the point was that if you have a replacement part or something that has been tested to requirements and you know it meets a standard, that's going to be better.

That really came up on the hoverboards. If you remember with all the hoverboard fires, that came up. Really a fascinating example of manufacturing in the 21st century. Hoverboard design suddenly rolled out and it was like the Wild West in having those built. We're buying hoverboards, and every time we opened one at CPSC, different circuit -- very similar circuit board design, but some were blue and some were green. They were just different enough.

The batteries were all the same shape. They were 2 by 10, meaning, like, 2 and parallel 10 in series. So there were 20 batteries in each, but every single battery pack was different. And you just pictured that literally they were going on their favorite bulk Chinese Amazon supply -- or supply site, not Amazon, sorry -- supply site buying things in packs of 1,000 and just putting them all together.

Sorry, long story to really just point out that as we were looking at hoverboards, specifically trying to make sure that the battery packs which were

causing the fires, which were the hazard that we were really worried about, fires, at CPSC at the time, making sure that they were being tested to a standard.

MS. WACK: Nathan, I'm sure we all remember a couple of years ago when cell phone batteries were exploding on airplanes and now we're hearing about it with vaping devices and issues with hoverboards. These things can really hurt people. And not everyone will do their due diligence to make sure they are making repairs safely, to the extent that they can be safe.

Putting aside repair professionals, do you support consumers being allowed to fix anything and everything?

MR. PROCTOR: So it's an interesting question. And George kind of raised this. Like, you know, who should do it? And then there's another question which is, whose decision is it to make what people do? And there are a lot of different options for that.

The option I do not accept is the manufacturer decides, after selling something to somebody, what they can do with it. If the FTC or the Consumer Product Safety Commission were to come in and say, these are particular devices that have some kind

of safety things and then there is a licensing program, which is hopefully -- I mean, we talked a little bit about authorized service.

I mean, if you say the only parts that are good are the manufacturer parts and then you refuse to sell the manufacturer parts and then you ask the Consumer Product Safety Commission to ban the use of any non-OEM parts, you have just required the Government to set up a monopoly for you. And that's a little bit unacceptable to me.

So who should decide? I think that that's a good question, but there is other elements to this, too, which is how it is accountable to the public. Who gets to decide what products are fixed in what way? That balances ownership, a free market for repair, and safety. Those are all things which we should care about.

But the solution being let's monopolize the repair process because this benevolent monopoly will protect consumers, yeah, I'm not a big fan of that particular line of reasoning.

MS. WACK: We heard from both Jennifer and Theresa about how these repair restrictions have affected their small businesses. Walter, 80 percent of the members of your organization, CTA, are small

businesses or startups. What impact would opening up this repair ecosystem and requiring devices to be repairable have on those organizations' ability to innovate and their bottom lines?

MR. ALCORN: Yeah, I think it varies. Honestly, for manufacturers, I think it would have a pretty significant impact. Most of CTA's members are -- actually, the majority of them are not manufacturers. They're either installers of consumer electronics devices or retailers. We have also technology-based companies. We also have ridesharing companies. We have lots of different companies that are focused on consumer technology, either as a technology provider or as a manufacturer of technology.

So I think it's hard to generalize how the impact would be for CTA overall. But I would point to the companies that show up at CES, which are -- at least the ones that exhibit are overwhelmingly manufacturers. And this is one of the few issues that I've heard from many, many, many manufacturers about in terms of concern that some of these state bills would be enacted. I have heard concerns that range from everything that's more practical, how the heck would I provide all this information to everybody who

asks; I've heard concerns about long term -- about liability. Who's responsible when an unauthorized repair provider does do something wrong based on technology or based on software that was provided by the manufacturer that enabled them to get in there and do the wrong thing?

I think it would be a big change that would be instigated, as been proposed, by the Government. And I think that just because we're talking about a new government mandate, it's something that we should all pause a little bit and make sure that we've thought through the consequences, that we've worked out these details.

I don't even think we've really gotten very far in that conversation at this point. So I have a hard time coming to a bottom line, but there would definitely be an impact.

MS. WACK: Walter, you mentioned unauthorized individuals getting in and making maybe shoddy repairs. Does CTA have any empirical data that shows that authorized repair providers perform higher quality or more secure repairs than owners or independent repair providers? Is that something that's been studied?

MR. ALCORN: I'm not aware that anybody has

studied that. I would presume that given the fact that these manufacturers, who put the most time into authorizing repair providers -- these happen to be some of the brands that are the most valuable in the world -- they want to make sure that whoever is working on their behalf is doing a good job.

Whether that actually happens, I don't have any data on that. I sure hope it does. There are probably a lot of shareholders out there that hope so, too. But that is one thing that -- that's probably yet another thing that hasn't yet been studied.

MS. WACK: Theresa, many third-party repairers will just become certified by an OEM. Why isn't that sufficient? Are you still limited in your ability to conduct repairs even if you're certified?

MS. MCDONOUGH: Well, I'm not certified by any OEM. The reason being is I don't find it necessary. I want to work on all devices and not just be considered, like, an Apple repair specialist. In our state, there is only one Apple-certified retailer and they don't work on phones and they don't work on tablets. And there is no Apple store. So to me, I really don't see a benefit in picking one over the other.

And even having that training doesn't

necessarily -- we were talking about this earlier -- mean that you'll get certified. You can spend $2,000 for their training, which I bet I already know most of it just because I do it every day. You know, maybe for somebody starting off, they might think that it's a benefit. But I've read some of the requirements that these companies have. You have to have a line of credit. You have to have a certain amount of employees. Like the list is -- the bar is very high. And for a small business, when you live in a state of 600,000 people, I just don't see it as beneficial to spend that sort of money on a certification that I already think I have.

MS. WACK: Jennifer, for you, you're an IT professional, you're engaged in technical and specialized work. Does that make a difference as to whether you should have access to information on repairing certain kinds of devices? Like should there be a litmus test for --

MS. LARSON: For my technicians?

MS. WACK: Well, for your technicians, yes. But if you are dealing with a highly technical device, is that something where there should --

MS. LARSON: We deal with very highly technical devices and we aren't authorized. But I

would say, any good business owner who wants to keep their brand and reputation is going to make sure they have technicians that can repair appropriately. My technicians go to training like certified technicians. They do certifications, but they aren't certified through IBM, per se.

But we work on high-level EMC, Hitachi all the time. And in 20 years, if I didn't have good people, I wouldn't still be around. So I don't know if that answered your question specifically.

MS. WACK: Well, sort of. My question is, also, when you're dealing with these highly sophisticated -- you're dealing with a server, should anyone be allowed to get in there or do you think that the companies should be able to say you need to have a certification?

MS. LARSON: Oh, no. I'm with Nathan. If you buy it, you own it. You should be able to do whatever you want with it. I own the equipment. It's my inventory. I can say, you know, to whatever technicians I want to work on it. But, absolutely, it should be a free market, it should be my product, and nobody should be telling me what I'm going to do with it.

MS. WACK: Nathan, one of the points in your

PowerPoint was that manufacturers design products without considering repairability. But what leads you to believe that repairability is something consumers care about?

MR. PROCTOR: Yeah, that's a good question. I want to quickly follow up on some of this "authorized" conversation because I feel like we're misconstruing the point a little bit, which is the authorized process is not a technical training.

MS. LARSON: Right.

MR. PROCTOR: To construe it as that would be to fundamentally misrepresent it.

MS. LARSON: That's good.

MS. MCDONOUGH: Right.

MR. PROCTOR: The authorized process is a business relationship between you and the OEM. So the question is not, do you want training on how to fix these things. The question is, do you want to enter into a relationship with this business, which has a whole set of contractual obligations. So it's much bigger than the training. I just wanted to make that point.

MS. LARSON: Right.

MS. MCDONOUGH: Yeah, yes.

MR. PROCTOR: I would say that, yes,

consumers lack information at the point of purchase about repairability. And so it's difficult to look at consumer behavior at the checkout line and say, okay, these people -- you're making all these different determinations about what you want when you buy something. And then you find out much later that the repairability is an issue.

And then you come to somebody like your friendly consumer advocate and you write an angry email saying somebody should stand up and fight these guys because -- you know, Paul Roberts was just telling me he bought a $70 Logitech mouse and the whole thing is epoxied together and the battery went after 18 months. And he didn't know that the whole thing was -- how could you know if you were at the checkout line? This looks like a high-quality piece of electronics. It's epoxied together; it's essentially a disposable product. Luckily, he's got some friends who know a lot about fixing stuff so he's going to get some advanced epoxy-undoing techniques. But, you know, this is a problem.

You know, Consumer Reports had a series of Dyson vacuums which they reviewed really highly on their initial pass, and then they had to reduce the Consumer Reports ranking after they got, you know, a

couple years out when that found that consumers started reporting in mass numbers that these devices break down and are unfixable.

So I think the problem is the point of sale is just -- consumers don't have enough information and then we're trying to like -- I mean, people are trying to crowdsource that information, but that's a problem now. You know, you can't say the consumers don't want it because I hear those complaints all the time.

MS. LARSON: Yeah.

MS. MCDONOUGH: Yeah, they do want it.

MS. WACK: Walter, manufacturers assert that many of these methods, including the epoxying of parts together, that are often discussed as repair restrictions are, in fact, just design decisions that are necessary to meet consumer demands for smaller, thinner, and more secure products. What effect would right to repair have on those sorts of decisions?

MR. ALCORN: Well, thank you for asking that question. I actually was hoping to get in on the consumer demand issue. I think if we're talking about a requirement that -- well, I think it depends in large part on what exactly would be implemented. I think it's hard to generalize because there are a number of different components that have been put on

the table in terms of legislative or regulatory fixes.

I think, in general, it's safe to say that it could have a negative impact on innovation, and here's why. We've heard problems of batteries being glued in. My understanding, and I've talked to a number of manufacturers about this issue, we're seeing batteries glued in for a couple of reasons.

One, there is the issue and the concern about the wrong battery being put in upon replacement, which creates safety problems. Thermal events, I think as some people call them. But then the other issue, which is a significant issue, is consumer demand. If you actually have a battery that's fully integrated, say, into a smartphone, you can put a much thinner battery in there, which means you get a much thinner phone. That's what consumers are buying.

And, now, it's moving to other products. We're starting to see this. I'm not saying this is good for the repair industry, but this is being driven by consumer demand for slimmer, sleeker products that have the functionality. I mean, I think we are seeing advances in some ways and then challenges being created on the other side. So consumer demand is something that these manufacturers spend an awful lot of time and money trying to figure out and they

compete fiercely for that.

I wish there were more demand from consumers for environmentally related attributes. In this country, we just have not seen that harnessed by anybody. And if there's entrepreneurs in this room that can figure out a way to do it, I'm all for you.

MS. WACK: Speaking to the question of environmental effects, Theresa, you said that over 400,000 smartphones a day are being recycled. Where does that come from? Where does that number come from? And does that number include phones placed on the secondary market?

MS. MCDONOUGH: Yeah, I think that was actually --

MR. PROCTOR: It's an EPA statistic.

MS. MCDONOUGH: Yes, I think I got that one straight from Nathan on NPR.

MS. WACK: Walter?

MR. ALCORN: Yeah, that was an EPA statistic in one report about 15 years ago. You can't even find it on the EPA website. You have to go to their archives in order to find that number. And the reason that you can't find it is it's not a good number. 400,000 phones a day -- if you did the sloppy math and you assume that every phone that went out of service

was thrown away, then, yeah, that might be a pretty good number. But that's just not the case.

At CTA, every couple of years we do a consumer recycling and reuse survey. And one of the things that we ask is, what do you, as a consumer, do with your old device whenever you're done with it? Well, the overwhelming number of consumers that responded to our survey say that they donate them to friends and family. And then beyond that, you recycle them. There are other things that people do. You get down to "throw it in the trash," for smartphones in particular, 1 percent of all consumers that got rid of a phone last year, which is about a quarter of all consumers, said that they threw it away. That is a heck of a lot lower than 400,000.

I've seen that number around. It drives me nuts. This is actually the type of thing that I go to state legislatures and talk about. Because there may be reasons to have repair legislation, this is not one of them. Don't buy into that one.

MS. WACK: Nathan, it looks like you had something to say?

MR. PROCTOR: Yeah, I have a couple of points to make on that. So the UN World Economic Forum said in January that electronic waste is the

fastest-growing waste stream in the world. We know that electronic waste is a huge problem. And it's true that the 416,000 cell phones which enter the waste stream every day are not literally going into dumpsters. But let's talk about cell phone recycling because this is the solution manufacturers say, we recycle these things. But how much of the commodity value of a cell phone is recouped in that process? And how much is that worth versus how much is a used cell phone or a repaired cell phone worth? We're talking about an enormous drop in value.

The iPhone 7s, when you drop them, the audio CODEC chip sometimes pops off. It creates this thing called "boot-looping." I'm sure that Theresa's seen this many times in her store. This chip is tiny. It weighs a fraction of a gram. If you are under AppleCare and you take your iPhone 7 with a boot-looping issue to Apple, they will give you a refurbished iPhone. And maybe that's good. But if you take it to an independent technician and they replace a tiny fraction of a gram component and restore 99.9 percent of the material value of that phone, that's like recycling at 99 percent efficiency. The best electronics recyclers in the world are nowhere near 90 percent. In fact, Apple brags -- and

they have invested incredibly in their recycling -- it's 40 percent material recovery.

So maybe 25 percent of the cell phones are effectively recycled and 40 percent of those materials are recouped. Ecologically, repair is just, in order of magnitude, more important for the environment than recycling.

MS. LARSON: It's not just cell phones. I'll make that point.

MS. MCDONOUGH: Yes.

MS. LARSON: My servers and the chassis that are going into the scrap are huge and enormous and it's only getting worse, all of our switches that can't be resold. I mean, I can't even fathom how much that's grown. I should probably try to see if there are statistics on it.

MR. ALCORN: Yeah, just one point, and I think this is a really good discussion. Thanks for getting on turf that I can talk. The one thing I forgot to mention, and this does go back to smartphones, how many people in this room have sold your smartphone or traded it in for credits? How many folks have done that?

MS. LARSON: I just did that.

MR. ALCORN: Okay. Many, many of us have

done that. That's actually what's driving this. Nobody pays to recycle a smartphone. That's all going into the reuse market. And the point there is, the way many of us see this issue -- on some products, not on all, this is a battle about who does the repair, not where the repair is done.

I totally agree with Nathan. Repair is better than recycling. We want to see more repair done. But let's not conflate no repair with who's doing the repair because they're really two different issues.

MS. LARSON: Can I make a point that repair has a lot of different meanings? Like when I'm repairing and I need firmware, that's a repair to make it work with other equipment. This is so much broader than just repairing cell phones. I understand this is a consumer panel. But, overall, this goes from everything like we've talked about, small consumer items all the way up to tractors like we said.

So I just want to remind people that some of the issues like tying and the licensing, that all goes into this. It's not just can I open up a cell phone. I just want to make that point while I'm up here because that's my business.

MS. WACK: That actually leads well into the

next question I was going to ask, Jennifer.

MS. LARSON: Okay.

MS. WACK: You mentioned that -- well, you just said that a lot of the issue that you face with repair is updating the firmware. And that when you can't do that, then the device just needs to be thrown away. But we've also heard about security concerns that allowing third parties access to that sort of information could cause a cybersecurity threat. Can you speak to that?

MS. LARSON: Yeah, we don't want anything deeper than just diagnostics and firmware patches. It's just like anything else. We don't want to get into the software, none of that. I just want made available to me what authorized dealers get.

When I buy a server, I buy firmware with it. So I should be able to get the updates needed to make it connect to other software. In fact, I was reading last night that this Mozilla FTC filing said interoperability is a powerful key to unlock competition in the tech sector. I'm talking about interoperability -- operability, sorry. And the idea that I have a machine that I own and I bought the firmware with it, but now to make it connect to new equipment I have to have a maintenance contract,

that's just wrong and anti-competitive.

MS. WACK: Walter, you were just discussing that the question isn't necessarily whether things get repaired but who does the repair. But what about instances where the OEMs are just not interested in engaging in repair? You know, if it's more than just a broken screen or a battery, why should that not be something that's opened up to third-party repairers or to consumers to be able to repair those devices?

MR. ALCORN: Well, I think it's a good question as it relates to maybe the low end of the market for many product categories because -- and, again, my knowledge is on the consumer side, not the B2B. But at least in the consumer market, manufacturers that are active in CTA's process, all have some form of repair capability they provide to consumers. So we may, but I don't think we represent the manufacturers of those cables that are sold in gas stations, maybe somewhere. But I know for the brand names, they do all provide some sort of repair option to consumers. Now, it varies considerably. We have some companies that have gone out and literally authorized thousands of repair facilities.

We have others that basically have very few options or they want you to mail it back in order to

get it repaired. So I'm not saying it's perfect, but what I've seen is, at least, the more valuable the product, the higher end of the market, the more those companies are focusing on repair and making sure that consumers have the ability to get it repaired at authorized places.

MS. WACK: Theresa?

MS. MCDONOUGH: Can I just make a point to that? Basically, that sounds idealistic in a way. When you live in a state where there is no Samsung, no Apple store, how many of you could be without your phone or computer for three or four days when you run a business or you do your work on it? Not very many of us.

So having the ability for small shops like myself to fix these devices is so important because most states or rural areas don't have access to quick reliable repair shops that are certified Apple or certified -- well, I don't know about Samsung. But it's vital that you have these small shops because otherwise people are going to be forced to upgrade because they can't be without a device for very long.

MS. WACK: We have a question from the audience for Nathan and George. With the future of cars and software controls, how can we be sure our

computers are safe before we're sharing the road with others?

MR. PROCTOR: "Our computers are safe." That is an engineering question for the manufacturers. And a lot of these repair conversations sometimes are really engineering questions for the manufacturers. They design and deploy devices that function a certain way and they make certain engineering choices that implicate the cybersecurity of those devices and the repairability of those devices. And, yeah, I think that there should be hard questions about the trade-offs that are being made.

And the standards especially for things -- like, we have really good product safety standards for airbags. But what about our data security in a car or what about, like, I mean, people who are driving their Tesla and then it has a failed firmware update halfway through and the car pulls over because it needs to flash the firmware and you were driving?

I mean, I think that there are problems that we're experiencing we haven't experience before. And I think it's good to engage in those problems, but those are engineering problems at the manufacturing stage.

MS. WACK: So my last question is -- I'm

going to end with you, Theresa, as well. So in one of Walter's slides, it said that the right to repair bills that have been introduced in the states would require device manufacturers to allow anyone to change or enhance their devices, on top of just repairing them. So you've supported the Right to Repair bill that came up in Vermont. Is that an accurate characterization of what you were supporting, the ability to change and enhance?

MS. MCDONOUGH: So few people even -- I mean, my mother can't even reply to a text message. So for the average consumer to want to enhance their device, that's only for a few techie people out there who want to customize and flash their device. The average consumer just wants to be able to use it.

The right to repair bill is not really -- you know, we don't want to have to change the actual software of the phone. We want to just have access to fix our phones. We want to have access to good, reliable parts. And, yes, most phones do get passed down, but I can guarantee you a good majority of you who've passed your phones down have also had to have them repaired because you've broken them.

So the Right to Repair bill does encompass all that, but particularly why I -- you know, yes, it

is my career. I want to be able to have a job 20 years from now. Who knows where technology will be, but it's not that we want to recreate the wheel.

MS. WACK: So I hope you'll join me in thanking these panelists for their time.

(Applause.)

MS. WACK: Our second panel will be beginning in just a few minutes. Thank you very much.

PANEL 2: WHAT ARE THE ARGUMENTS FOR AND AGAINST REPAIR RESTRICTIONS?

MS. TODARO: Thank you, everyone. If you all could take your seats again, we'll get started with Panel 2.

Thank you. My name is Christine Todaro, and I'm an attorney in the FTC's Division of Marketing Practices within the Bureau of Consumer Protection. And I have the pleasure of moderating this Panel 2, which is focused on the arguments for and against repair restrictions.

As a reminder, please silence your cell phones and any other noisemaker you may have on you. And as with the prior panel, if you have any questions, please write them down on a question card and FTC staff will come and collect them if you raise your hand, and then those will be brought up to me.

As you'll see in their bios, I'm joined by four esteemed panelists. Gay Gordon-Byrne is the executive director of the Repair Association. Dr. Gary McGraw is a security researcher and supporter of securerepairs.org. George Kerchner is the executive director of the PRBA - The Rechargeable Battery Association. And Dr. Earl Crane is a security advisor for the Security Innovation Center.

I've asked each panelist to give a brief seven-minute statement on their position of the right to repair. So we'll start with Gay.

MS. GORDON-BYRNE: Sure. Hi, everybody. Gay Gordon-Byrne. I'm the executive director of the Repair Association. We're actually formerly the Digital Right to Repair Coalition, which is just a mouthful, so we call ourselves the Repair Association.

We formed ourselves in 2013 in order to drive legislation that would be repair friendly, because we were noticing monopolies of repair in just about every market we ever looked at. We've also been working with standards groups and regulators, the US Copyright Office, and some international entities to try to do similar things for the benefit of restoring our options as owners of equipment to be able to repair the things that we purchased.

Monopolies on repair are, unfortunately, the new normal. We used to always be able to fix our stuff. It was a right of ownership. It still is a right of ownership, and we've lost it because we've failed to pay attention to all the nasty little things that were happening around us, such as the presence of end user license agreements, the degradation of contract to the point where Magnuson-Moss was being

ignored very broadly, lots of antitrust questions about whether or not you can tie a service contract to a purchase, and things along those lines.

So I just want to remind everybody repair is legal. It has always been legal. Repair is not how people violate copyrights. It's not how they steal patents. It's not how they acquire trade secrets. It's not how they hurt customers. And it's not how they violate cybersecurity. So I hope that we'll be able to talk through some of those issues here on this panel.

Now, the reason that repair monopolies are so prevalent is the number one thing is they're extremely easy. Manufacturers basically do nothing. They do less than they used to do in order to monopolize repair. They used to print instruction manuals and repair manuals and schematics and ship them with the product. Soon as they could post them up on the internet, they no longer had to print and ship. It was a cost savings.

The more stuff they got put up on the internet was a cost savings. And then some bright light -- I don't know where -- said, hmm, we should password protect this. And then somebody said, even better, we should charge for it. And then the final

bright light is, we shouldn't let anybody see it.

So it's cheap and easy for manufacturers to monopolize repair, which is a triple win for them. Because once they monopolize repair, they can charge anything they want and you're stuck. Consumer Reports did a study, it came out in 2014, and they advised their entire membership that if the cost of repair is more than 50 percent of the cost of a replacement, buy the replacement. It's horrifying to say that that was good advice, but it was good advice.

So they get to charge anything they want, and amazingly enough, repairs are now roughly 50 percent or more of the cost to replace the device. It's almost uniform. If a refrigerator is $1,000, repair is $500. It sends you into the showroom, and that is the intent. So the main benefit of all of this accrues directly to the manufacturers in every single way possible.

And the holy grail of all of it is to send you to the showroom to buy another product. And if they can then turn around and say, and I'll give you a great trade-in, which no one else can do because, by the way, they've also destroyed the used market, it is a perfect cycle of monopoly. And I hope that the FTC and some of the other regulators view it as the

monopoly that we see it as, because every aspect about it is unfair and deceptive.

So here's what's going on. You buy something, you go to the store, you own it until you turn it on. Because now those little end user license agreements say, they're active when you turn it on. There's no counter-study. There's no negotiation. There's not even a click to accept anymore. It's over. You turn it on, you've agreed to these ridiculous contracts.

And if you actually took a look at the contracts -- and I did -- and I did and provided it to the FTC as part of this panel -- basically, 100 percent of manufacturers have restrictions on repair in every one of their contracts. There's maybe one company, a company out of Europe called Fairphone. Their contracts are a little hard to find because I can't even find them. They may not even have them. Everybody else has the same language that says, you can't do this; you can't do that; you can't open the device; you can't upgrade it; you can't demanufacture. You can do nothing with this.

Now, this is totally incompatible with ownership, which is where the real problem is for consumers. We expect to be able to fix our stuff.

And we don't need any secrets to do it. We just need exactly the same information that the manufacturer created in order to fix their stuff under warranty. Because guess what? It costs them money to make good on a warranty, and that information is public knowledge.

The average in the tech industry is about a 5 percent accrual for them to be able to actively deliver on their warranties. So if their costs -- they basically said, on a $1,000 product, I need to make sure that my warranty cost is no more than $50. You better believe they've created the diagnostics, the procedures, the parts, and the tools that make that 50 bucks happen. But that's the information that they will not share. It already exists. It costs them nothing to deliver it. It's already out on a website. It's just the access to the website has been removed.

So that's the framework that I'm looking at. I think the answer to the basic question is, why is repair being monopolized? It's just money. If you dig in any one of these corners, you will find a pot of money. So, thank you.

(Applause.)

MS. TODARO: Dr. McGraw?

DR. MCGRAW: Hi, everybody. Pleased to be here today. I'm a security guy, which is odd, because it makes me sad. Because everything is insecure. And I've been working for 30 years to try to make stuff less secure, mostly by building it properly and designing it properly.

So what's that got to do with being able to repair something? Well, it turns out there are some lessons that we can draw from engineering -- and security engineering, in particular -- that apply directly to this repair thing. And that is as follows: If you think about repair and you have the capability to repair as part of your design requirements, you can create a system that is repairable. And in fact, we have lots of examples of those, because for many, many years, things were able to be repaired, even high-tech things.

Same thing goes for security. If you think about security while you're building something, you end up with a much more secure design than if you try to tack security on at the end or, God forbid, pretend you have security by putting security on your box without actually having any security. And if we design things to be secure, they're often much better than if we just sort of hope that things are secure or

we just connect insecure things to the internet.

The bad news about these two things that are related is that we're not so great at security engineering right now. We do have a problem with insecure devices. We do have a problem with insecure websites with software that's insecure, with cars that are insecure. And the internet is working its way into everything, as is software, so we can expect more insecurity. That's why I'm sad.

But if we work on security and, at the same time, we think, gosh, one of the aspects of being secure is being able to be fixed and changed and evolve over time according to the threat model that's out there in the world, then we can have, as one of our design constraints, the idea that people should be able to fix their stuff.

In fact, I think if a software manufacturer came to you and they said, well, we're just giving you this software and you can't change any bits ever for any reason, and, oh, by the way, there are these massive security problems that come and we're not going to fix them and you can't fix them, so nobody can fix them, so we're all stuck with this broken stuff, do you think that would fly in the high-tech software world? It would not. It would not. We have

to be able to fix things. In fact, security demands that we be able to fix things.

So the question is, who should fix things? Should it just be the manufacturer that sold you that stuff? Is it okay to count on monopolies, in some cases, to control the right to repair going forward? I think the answer to that is clearly no.

But I do think that free markets are things that we should strive for and we have to support the free market. It is fine with me if a monopoly decides we're going to say this is not repairable, and we're going to sell it as something as-is forever, doesn't change, here you go. And we, as consumers, can decide whether that's good for us or not.

You know, we may decide that's fine. I'll just throw it away and get a new one. That's a consumer decision. But, you know, if a company decides they want the right to repair to be built in, like security is built in, and they can advertise that fact and compete in a fair market, then we've got something better.

This does not speak to the third-party markets that we heard about this morning in the other panel. I think that's also important, but I think that the main gist of what we've got to get to today

is how we can tease apart this spurious security argument that I've heard out there in the world and the repair argument. Because mixing them together is a very sneaky trick, but it's not really true at all.

The truth of the matter is we can design things to be repairable, we can design things to be secure, and those things are not orthogonal. And that's all I've got to say.

(Applause.)

MS. TODARO: George?

MR. KERCHNER: Well, Gary's the security guy and I'm the battery guy. So I'm here to speak to some of the battery issues that were mentioned in the panel earlier today, but also give you a little education on the lithium-ion battery and cell world and how these batteries are designed to power certain consumer products.

So I'm with PRBA, The Rechargeable Battery Association. We're based here in Washington, DC. We represent the major manufacturer of consumer and industrial rechargeable batteries, as well as the products that are powered by these batteries. So everything from a cell phone to an electric vehicle to a 40-foot container that's used to hook up the electrical grid, our members manufacture those

batteries and those products.

As we know, lithium batteries -- lithium-ion batteries, that is -- is the preferred rechargeable battery for consumer products. We are committed to the safe transport, use, recycling, and disposal of these batteries. And we actually would like -- we're here to discourage new rules or policy from the FTC relating to right to repair that would exacerbate the fire risks arising from this mishandling.

So, again, PRBA's focus over the years working with the Department of Transportation, OSHA, Department of Energy, EPA, is all about the safe use, recycling, and transport of these batteries. So when the right to repair issue came up, I've attended some of the state -- I've testified in some of the state houses on batteries. And I've gone there to explain the difference between a lithium-ion battery or a lithium-ion cell and an alkaline battery.

So we, the consumers, can go to any store and buy an alkaline battery that we're all very familiar with, right? You can buy that at any consumer -- any retail store. When you go to buy lithium-ion batteries, or lithium-ion cells, as we say, we have cells, individual cells like, these 18650s and we also have things called pouch cells.

Now, I know the folks that are here that do repairs are very familiar with these pouch or polymer cells. They're very thin. They're flexible. And these are the types of cells that you see in a lot of your cellular phones, okay? The 18650 cells are used in things like power tools. They're also used in laptops and they're used in a lot of industrial products. So, example, some of the electric vehicle manufacturers will use, literally, 5-, 6-, 7,000 of these individual cells to power their vehicles.

The bottom line is, though, these cells, when they are electrically connected to form a battery like you see here -- so again, I've got five individual cells that are electrically connected for this power tool battery. This power tool battery is designed with a system in mind. That is, the battery talks to the charger; the charger talks to the device. It's a safety system when those devices -- when that entire system is tested.

So, for example, that battery is tested. The drill is tested. It's tested to a safety standard. And that battery was specifically designed to power that -- for example, in this case, a power tool.

When you go into the store and you buy a AA

Duracell or Energizer battery, that's a swappable battery. You can put an Energizer and a Duracell in the same flashlight, it will work perfectly fine.

If you take one of these cells out of this battery pack and swap it with another manufacturer's 18650 cell, that is a completely different battery design, okay? And that's an important thing to recognize, that these cells that are electrically connected in this battery are designed specifically for that particular product. It's not like you can walk into a retail store and buy an over-the-counter polymer cell like you see here, okay? This polymer cell was designed specifically to power a particular product.

So again, it's important to recognize from a safety standpoint -- and that is our focus at PRBA, is the safety of these batteries. We've recognized that they're used widely by a lot of consumers. They're designed to power specific products and they're also designed to be repaired by repair facilities that have been trained on how to replace these particular batteries. If you were to take one of these cells and pull it out of this battery pack without the knowledge of how that whole system works, that safety system, you're jeopardizing the design of that particular

battery and that particular product when it's used.

So, for example, these two cells look exactly the same. They have the same dimensions. They're 18650, 18 millimeters in diameter, 65 millimeters in length. This cell could have been designed to power a notebook. This cell could have been designed to power a power tool. If you mix these up, while they are the same size, and you put these batteries with these cells together, that's where we're concerned on some of the safety issues when consumers or repair facilities are unaware of the difference between these individual cells.

And I think that's important, at least from our perspective, where we have members who have as many as 30 different models of 18650s. One of our members, for example, the military came to them and said, can you make me an 18650 that I can use in very cold temperatures and high altitudes in Afghanistan? So again, that manufacturer went and said, okay, we'll make an 18650 cell specifically for that application.

And that's important to recognize, that when you're going in and you're repairing products and you're not aware of the differences between the different cell chemistries -- and there are about six different lithium-ion chemistries in the world today

that are used, both for consumer and industrial products. There's different chemistries. There are different designs to power certain products. And without that knowledge, there's a lot of safety concerns that we, as an industry, have.

And I think that's particularly important for the FTC and others to recognize that ubiquitous nature of lithium-ion batteries. We know they're out there. They're in hundreds, if not thousands, of different products. But understanding the safety issues associated with batteries and the different nuances with different chemistries, that's our biggest concern.

Let me see if there's anything else here I wanted to touch on before my time's up.

I think this was mentioned earlier. Our members do have repair facilities and they're authorized repair facilities. And as it was mentioned earlier, these employees that work at these repair facilities go through very extensive safety training, technical training. They have to pass software exams, hardware exams. And they're also trained on what happens if a battery goes into thermal runaway.

Now, I know somebody mentioned this earlier. You know, these batteries, if they're badly damaged or

they're improperly manufactured, they can go into thermal runaway. Temperatures when they go into thermal runaway, over 600 degrees Centigrade. So 600 degrees Centigrade for somebody that is not aware of the risks associated with that is a very serious issue.

So again, focusing our attention here on the safety issues, again, is the key thing for at least when we come into this right to repair issue. And, unfortunately, we have seen a number of incidents involving these batteries in transportation and use. Someone mentioned earlier the hoverboards, right? That was certainly the poster child of a badly-designed product, a badly-designed battery, and cells that were not properly designed to power that particular product.

And I hate to pick on the e-cigarette industry, but I'm going to have to, because that's another example of an industry that is misusing 18650 cells that were never designed to power things like a vaping device.

I'll leave it at that. My time's up. Thank you for the opportunity to speak, and I look forward to the questions.

(Applause.)

DR. CRANE: Good afternoon. My name is Earl Crane. I'm the other security guy, and that makes me happy because we have two panelists up here to talk about security in this important conversation. And I think what you'll find what's going to be interesting is Gary and I, by the end of this, are going to be agreeing on more things than we may be expecting so far.

So I'm going to go into it, and I'll apologize up front, I am going to go over my time. But I cleared that one already, right? Ask for forgiveness rather than permission. I've been in the field for 20 years. I'm a cybersecurity executive, and I'm an advisor to public and private sector organizations. And I've worked with security startups. I was at the White House on the National Security Council as a director for federal cybersecurity policy. I've worked in the financial sector and other Fortune 100s.

I'm also an adjunct professor at Carnegie Mellon, where I've taught cybersecurity to graduate students and executives since 2002. And I'm a cybersecurity fellow at the University of Texas - Austin Strauss Center. And, interestingly, for this conversation, back in 2010, when I was at Homeland

Security, I was part of the task force where we helped to bring consumer devices into government, called "bring your own device."

As you can imagine, my entire perspective is viewed through the enterprise cybersecurity lens. I also personally want to say that I'm a tinkerer and I am a fixer, and I appreciate the ethos of the repair movement. I will admit it's very satisfying, the feeling you get from repairing something you own and helping others who want to repair their broken things to help reduce cost, reduce waste, and help hardworking Americans stretch their dollar.

However, there is a big misconception that this is without consequence. Specifically, it can cause harm to someone else. And that gets to the core of my concern. Forcing repair on third parties, like enterprise customers and manufacturers, can make security worse and not better for all of us. And here's how.

First is the loss of accountability for security. It's difficult to hold OEMs accountable for security of their products if we also legislate design changes that will negatively impact security. Second is the risk of backsliding the security progress that we've made. It's not just a consumer security issue,

because we've merged consumer and enterprise technology. We can't think narrowly about how consumers use technology today, but think of how all of us will use technology in the future as our lives are interconnected and digital, both at work and at home.

And third is the loss of consumer choice in increasing costs. Consumers should have the choice to determine what design decisions are most important to them. Maybe it's safety, security, repairability, reliability, cost, and other features. The more constraints, though, we add through legislation, the higher the cost.

So first, I want to talk about accountability for security. Consumers have an expectation of privacy and security. They believe that technology products and services should perform as designed. However, without accountability, we have no foundation of trust. And without trust, we lose integrity. In the issue of repair, unauthorized repair removes the accountability that a manufacturer had for privacy and security, because an unauthorized repair breaks the chain of trust in a digital ecosystem.

Some manufacturers have gone as far as to

remove their ability to access a device without user credentials to preserve that accountability. However, mandating design decisions runs in direct contradiction of policies that focus on manufacturer accountability. And any repair legislation without a consideration for security and the preservation of trust is a risk and a danger to both the individual and our enterprise consumers.

The second piece I want to get into is the cost, the backsliding of our security progress. I'm concerned that repair legislation that's not coordinated with security efforts, not coordinated in the design process, will take a step backwards. To understand how, let's rewind back to 2007. When smartphones were first coming onto the market, these consumer devices were not designed with enterprise security in mind. However, people wanted to bring them into the office and use their powerful features.

Fast-forward to today, and leading smartphone manufacturers have incorporated enterprise security capabilities into their consumer products. The cybersecurity industry has been working for years to improve security in our hardware and our software systems. For example, at Homeland Security we sponsored a Build Security In program to help develop

best practices and guidance to build security into every phase of the software and hardware design. This led to new efforts in security engineering by government, industry, and academia.

Thankfully, industry has increasingly embraced secure development principles, leading to a safer and a more secure cyber ecosystem. And government agencies like the FTC and DHS have asked manufacturers to take responsibility for product security. The Government expects electronics manufacturers to implement comprehensive privacy and security programs covering not only new products, but also legacy products, as well. And that is what they've done.

Take, for example, where the US Government has worked with manufacturers to improve security of their products so they can process government information. We see this in programs like the Commercial Solutions for Classified Use Program, called the CSFC, and the Bring Your Own Device policies, BYOD, that I mentioned earlier for unclassified systems.

We worked with manufacturers to encourage them to build security into their devices so they'd be secure enough for enterprises to adopt, and this was

hugely successful. The consumer market drove demand for the latest innovations, like cameras and connectivity and battery life, while the enterprise market drove demand for security, privacy, and management.

What we did not do was mandate new security features through legislation. We used other levers, like the Government's buying power and the buying power of the market and participating in that market. And the participation was left to be voluntary on the part of the manufacturer.

Now, while not all manufacturers have embraced these programs, the leading ones have. And you can find their names. They're publicly listed on the NSA website. Yet, with the proposals that we've discussed, it feels like we're taking for granted the progress that we've made. And now we're at risk of backsliding to mandate design decisions on manufacturers to open up a broad range of devices without regard of preserving their integrity model.

It also sets a troubling precedent for the future of connected product security and privacy. Forcing repair requirements onto devices that were not designed into the manufacturer's security model breaks the device integrity. The security capabilities will

be less effective, both for enterprises and for consumers. This is a big deal because it's a slippery slope. If design decisions can be mandated by government that compromise security and privacy today for repair, what's to stop future legislation from compromising security and privacy in light of some other goal that was seen as altruistic at the time?

Today's most sophisticated internet-connected device is our smartphone. What happens in 5 or 10 years when smart internet-connected devices are pervasive? According to Forbes, internet-connected devices will continue to grow at 7.3 percent annually, with industrial IoT projected to be at $123 billion in sales by 2021.

The same innovations that brought smartphones into the workplace will bring smart devices into all aspects of our lives. Not just our lives as a consumer, but the way we work, conduct commerce, and manage a global ecosystem will fundamentally change over the next decade.

And, third, I want to talk about consumer choice. Consumers should have a choice between a repairable device, a secure device, or a securely repairable device, each one with increasing cost at each option, because we're putting more constraints on

the engineering process. But forcing this option outside of the design breaks the security model and it breaks the market. Forcing repairability to trump security is short-sighted and will drive up the costs for all consumers as this new constraint is mandated.

We're at risk of taking away the ability for manufacturers to design their IoT devices for security and economic competitiveness, because we want dual-use devices for work and for play. Additionally, mandates for repairability and security will drive up the cost for dual-use devices that are both highly secure and consumer repairable. Consumers may not want to pay for both, and they should be able to make that choice for themselves.

Manufacturers make conscious decisions about what they release publicly, what they share with only their partner networks, and what they keep confidential. For example, many companies already publish their documentation and APIs publicly so organizations and individuals can build interfaces. Today, authorized shops and dealers that provide repair have an obligation that a repair is performed to manufacturer standards, addressing safety and security issues. Forcing manufacturers to share codes and tools that push beyond what is necessary for

repair inadvertently may cause harm.

In addition, it may also result in the information sharing environment that we've built for information security for partner networks to clamp down, inhibiting innovation, growth, and the sharing of security information. So consumers have plenty of choices in the marketplace and they can choose some manufacturers that prioritize security and others that prioritize repairability. But there's no reason that legislation should mandate repairability and take away consumer choice between repairability and security.

This is a complex issue. There are no easy solutions, but I'd like to reiterate my three guiding points. Don't give manufacturers an out of accountability for security by mandating they open up their devices for repair. Don't reverse the security successes we've already had and don't remove the consumers' options to get their devices repaired based on their level of informed risk appetite and their need for accountability.

Thanks for your time. I look forward to your questions.

(Applause.)

MS. TODARO: Gary, I'm going to start with you. How do you respond to Dr. Crane's argument that

design and security don't necessarily go hand-in-hand?

DR. MCGRAW: I don't think that's what he said. I think what he said is designed for repair and designed for security together would be so expensive --

DR. CRANE: It would be more expensive.

DR. MCGRAW: -- that we can't innovate.

DR. CRANE: I wouldn't say that we can't innovate, but you're absolutely right. We can design for security --

DR. MCGRAW: I'm just putting words in your mouth.

DR. CRANE: But I appreciate you correcting the question, was my point. Thank you.

DR. MCGRAW: So my view is that the cost doesn't necessarily have to go up if you have repair as one of your design objectives. So you may not have security as a design objective, by the way. That's not always important, and consumers can decide whether they want something secure or not. Right now, the problem is that consumers are woefully misinformed about a lot of things. Security is one of them. Repairability is another.

You sort of assume that you're going to be able to repair some stuff like, I don't know, a

tractor, you know. Because my father-in-law has 30 tractors in a tractor shed and they swap parts all the time. And they keep about five of them running for apple-picking time. And guess what? When that's no longer possible, that cuts into the tiny sliver of margin that farming already has. That's a problem. And we have to just recognize that that's a real problem and try to design around it.

I think that the real answer is that we can, as high-tech people, cooperate and think about both of these aspects that we may want and create products that can do both that may, in fact, even be cheaper and may serve to open other aspects of the market that would be otherwise closed because of monopoly.

So I do agree with your claim that having two constraints is more challenging. But I don't agree that that makes things more expensive. I just think we have to do it. And I think we should do it ourselves. That would be great. We have a really crappy track record on that, so it would be a super bummer if the FTC had to make us do it because we should just do it.

DR. CRANE: Do it ourselves.

DR. MCGRAW: So let's do it.

(Applause.)

DR. MCGRAW: Sorry, what was the question again?

(Laughter.)

DR. CRANE: But I like the answer.

MS. TODARO: You tell me.

DR. CRANE: I like the answer, and I'm happy to respond to any parts of it, too. But like I said, I think we're more aligned than different, as security folk.

MR. MCGRAW: So do I.

MR. KERCHNER: I should let these two sit together.

DR. CRANE: You're intentionally in the middle.

DR. MCGRAW: There are dangerous batteries between me and him. They might spontaneously combust. So I'm really worried about that.

MR. KERCHNER: Nobody wants to sit next to me when I bring these batteries.

(Laughter.)

DR. MCGRAW: Can you scoot over a little?

MS. TODARO: We're going to talk about those batteries in just a second, but Gay has something she'd like to say.

MS. GORDON-BYRNE: I just wanted to make one

comment for Dr. Crane, is that I'm very personally involved with all the bills that have been presented for right to repair in state legislatures. And the only bill that had any kind of design requirement in it, which was shot down in Washington State, was that there be no glue.

Our proposals and our philosophy is that we don't want to make any design requirements. If manufacturers want to make stuff that's unrepairable and glued together, that is a consumer choice. It's a design choice; it's a marketplace. The free market will resolve those questions. So I just want to please detach that right to repair legislation, as being proposed, is headed towards, in any way, a design mandate. Because it's not.

DR. CRANE: If I could respond to that, so I disagree. The legislation that I looked at, anytime you put a constraint onto a system that says it needs to meet a particular capability, that becomes a design constraint.

MS. GORDON-BYRNE: No, there's not a word in any of these bills that says that.

DR. CRANE: I saw elements describing how there were requirements for what manufacturers would release and the necessity to be able to have

components and parts within those bills that was more --

MS. GORDON-BYRNE: It does not. No.

DR. CRANE: -- it was taking it beyond repair. And the problem is that the bills were inarticulate.

MS. GORDON-BYRNE: Excuse me. Bring up a bill. Put it up on your laptop, and let's read through it together. Because you are making extrapolations about the language in the bill that are not there. They are, frankly, not there. And if there are things that are there that are offensive to legislators, they will be more than willing to help them and to revise the bill. But there are no design requirements whatsoever.

The only requirements of the bill is whatever the manufacturer currently makes available to its "authorized" locations. And that is only what they're required to provide, is what they've already created for purposes of repair. If they are selling a service assembly, they don't have to sell a component. They only have to sell the service assembly. If they are putting documentation out on the internet, they just need to make it available. It just needs to be the same. That's all it has to be, is the same.

MS. TODARO: I'm just going to interject here for a second. The third panel, the next panel, will be discussing some of the proposed legislation.

MS. GORDON-BYRNE: Okay, very good.

MS. TODARO: So if we can continue the discussion on the arguments in favor and against limitations on the right to repair.

MS. GORDON-BYRNE: All right. I'll shut up.

MS. TODARO: It's a very important discussion, but since there will be another panel that will specifically address some proposed legislation, I think we will move the discussion forward.

I'm going to turn a question over to George. There's been a lot of interest from the audience about the safety of these batteries, the lithium-ion batteries. And the question that several people have raised is, why don't the OEMs just release information about the different types of batteries to third parties? And if that information was out there, would that eliminate some of the risks of the physical safety associated with the batteries?

MR. KERCHNER: Yeah, that's a great question. Thanks for asking that. So I think the short answer is no. Because, again, last year, I think there were seven billion lithium-ion cells

manufactured last year, right? So having someone -- a consumer, for example -- understand the difference between that 18650 or the next 18650 or this polymer cell from another polymer cell is very difficult. And I think it was mentioned on the first panel, there's a lot of counterfeiting that's going on in the marketplace, right? So having that information -- just handing that information over to the consumer may not be enough.

In addition, because these batteries -- when you're electrically connecting batteries -- are designed as a system -- again, the battery's talking to the device; the device is talking to the charger. There's a lot of complexity there. And those batteries and those devices were manufactured to certain safety standards. And allowing consumers to be in there to repair those without that knowledge of those safety standards is a big concern for us.

In addition, and I have to mention this, that if a consumer repairs a battery, a multi-cell battery like this, that's a completely different battery design. And if that consumer takes that product or that battery on board an aircraft when they're traveling by air, that's a violation of US and international standards. Again, because that battery

design was tested to a certain specification. It's required by the Department of Transportation, international organizations. And any change to that design is going to be a different battery design. It's not going to be the same battery that was tested to a certain standard.

And in order to carry those onboard the aircraft as passengers, if it's an untested battery, that's a violation of federal as well as international standards. I just wanted to point that out.

DR. MCGRAW: Why do we want them again?

MR. KERCHNER: It's an awesome technology.

DR. MCGRAW: Oh, okay.

MS. TODARO: Gay, is there any evidence that supports the argument that parts used by independent repair shops are more likely to be counterfeit? Or what's your argument or response to an argument that independent repair shops are more likely to use products that may be counterfeit?

MS. GORDON-BYRNE: I wouldn't say so much counterfeit as I would say they may not be the same quality. And the reason is that if the manufacturers will not sell their parts, people are really highly demanding repair and they will seek out parts. And they will seek out parts on eBay and on all sorts of

-- any way that they can, because the manufacturers won't sell the parts. And this includes batteries, as well.

So there is no certification for parts, as was talked about earlier. There's no way for a consumer to know if a part has been blessed or not blessed. Just as in the auto industry, when you go into a dealership and they say, do you want an aftermarket alternator, an OEM original alternator, or a rebuilt OEM original alternator? You have those choices. In the electronics world, those choices don't exist.

If you can't buy the OEM original, which is the de facto situation right now, you're always buying a brand X, and you don't know how good it is. It's probably functional or you'll immediately reject it as a buyer.

Whether it's counterfeit, I can't speak to that. I know there's some evidence that there's a lot of counterfeit electronics. But that, I think, is more of a problem of the OEM policing their supply chain more effectively than they do.

But, basically, consumers want original parts. And if they can't get them, they're going to get a substitute. The quality is variable, and a lot

of our small repair shops have a lot of trouble acquiring parts. But in the enterprise scale equipment, they are acquiring parts off of existing technology. So they're taking it -- like Jennifer said, they'll take a power supply off of something that's not working for some other reason and they'll insert that. So it's an original part. It's an authentic part. It's just really hard to do with things that are consumable, like batteries and glass.

MS. TODARO: So, George, if the OEM parts were sold directly to the independent repair shops, would that alleviate some of the concerns that you have?

MR. KERCHNER: Well, again, not necessarily. If it's an authorized repair facility that has been trained in how to replace the battery, how to respond to thermal events involving batteries, understanding the entire safety system associated with that battery, that's the model our members support. Again, there are thousands of authorized service centers for the products that our members manufacture. They've gone to great length to train all those employees to understand how to properly install those batteries.

If it's installed improperly by an independent repair facility that's not authorized,

they could have installed it properly, but down the road, if that phone or that notebook or that tablet gets dropped and that battery gets jostled around, that's where the damage could come, especially for these polymer cells. And, again, this is the preferred form factor for all those thin notebooks and cell phones and such that we have. And it's flexible. There's some flexibility there.

If you damage that separator -- and again, in our comments that we filed with the FTC, there's a great example of a phone that was repaired by an unauthorized service center, where a screw was left inside the phone. It punctured the cell, caused a thermal event on an aircraft. And those are the kind of things that, again, we have to deal with.

And at the end of the day, if it's a lithium-ion battery incident, it's a black eye for the whole industry, right? It doesn't matter whose battery it was, if it was an Apple product or a Samsung product or an LG CAM product, whosever product it is, their name is in the headline, right? So we're very sensitive to the fact that our members are very supportive of the whole authorized repair facilities. And that's why they go to great length to train their employees to understand those safety issues.

MS. TODARO: Dr. Crane, can you talk a little bit more specifically about the cybersecurity risks that you see associated with third-party repair?

DR. CRANE: Fundamentally, if your -- so there are two key aspects to that. One is to the device and the other is to the design. So first to the device is if you are changing out any component at the hardware level with another piece of hardware, you're not able to provide the same level of assurance that something else didn't happen. So that's the first key piece of that.

And we've gotten a lot better with built-in security modules, TPM modules, signing keys on devices to try to protect those crypto devices, protect those secrets on the device, and making sure that the right integrity and relationships with those components are preserved helps to provide that security integrity on the specific device.

The second one is that it's a fundamental rule of security that the best security is -- like with a crypto algorithm -- that it's open to the public. It's open for inspection. Good crypto algorithms are those that are open for the public and for inspection. What's not okay is when you open up the signing keys, the secrets inside. And the

challenge has been that in the repair conversation, it has not been articulated enough. We haven't had enough of a security discussion in here to make clear what will be mandated to be released and where the overreach is. And that's why I'm glad that we're having this conversation now.

MS. TODARO: Gary?

DR. MCGRAW: I've got a question. So do you believe in free computation, that you should be able to compute stuff?

DR. CRANE: You mean -- what do you mean?

DR. MCGRAW: People. Like should people be allowed to compute things, run software, do computation or should that be controlled?

DR. CRANE: Well, it depends on what the computation does. Computation to calculate the nuclear control secrets, right?

DR. MCGRAW: Yes, good. So sometimes it does need to be controlled, and other times, it may not need to be controlled.

DR. CRANE: Yeah. It depends on what the purpose is and what you're doing.

DR. MCGRAW: So if we build a security model for a consumer device that is the same model we use for nuclear secrets, is that overkill?

DR. CRANE: It depends on what the cost is going to be, right? If a consumer device, that security module, can be computed and it's the same one that you're providing and it's purchasable for a consumer at the same price point, it's a good thing that it's more secure.

DR. MCGRAW: So I remember an iteration of this kind of conversation intellectually about, I don't know, the late '90s, when Microsoft was talking about putting a security code processor on some of their motherboards. And the thinking was, well, that's good for some aspects of security, but what if Microsoft decides that only Microsoft signed code should run on that platform because security? That's taking away computation freedom.

And at the time, that was used to push back against this overreach of a monopoly, at the time. And I think it was done properly. And, frankly, I think we're in the same place right now, where we're using security as kind of this shield for a land grab that is unnecessary.

DR. CRANE: Right. So the instance you're referring to was some of the restrictions where you wouldn't be able to run other operating systems on Microsoft hardware?

DR. MCGRAW: Other software at all.

DR. CRANE: Right. No Star --

DR. MCGRAW: It turns out other operating systems --

DR. CRANE: Yeah, no StarOffice, no OpenOffice, no Linux systems.

DR. MCGRAW: No Linux.

DR. CRANE: No Linux systems on those.

DR. MCGRAW: Now Microsoft sells Linux.

DR. CRANE: Right. So the issue is, while I think that's an important piece of the conversation when we're talking, I don't think that that's germane to the repair conversation. Because we're not talking -- what you're describing is being able to use software outside of the original manufacturer design specifications to have the openness to compute other things on it, as well. And that's a modification.

DR. MCGRAW: Because it was designed incorrectly.

DR. CRANE: That's a modification and an enhancement, not a repair to manufacturer standards. And it is a good and important conversation to have, but not part of the repair discussion.

DR. MCGRAW: Yeah. I think you and I agree that they can be orthogonal and they probably ought to

be orthogonal. So I get worried when we tie this notion of security as, oh, my God, that's going to break -- you know, if we add repair, it will break security. I think that's just indicative of really bad security design.

DR. CRANE: Right, and there's plenty of bad security out there.

DR. MCGRAW: Oh, man, there's --

DR. CRANE: Already, yeah.

DR. MCGRAW: I'm with you on that. So there's unwashed horribleness that we don't even want to talk about. But among the people that are trying to build stuff for people to use and be secure, we can make different decisions. And we can make systems that are able to be repaired and also secure at the same time.

DR. CRANE: And we've had a lot of successes in doing that as security engineering processes and security engineering -- I mean, a lot of the seminal work that you've done has been very helpful, right?

DR. MCGRAW: I did that?

DR. CRANE: Your top 10 security things that need to happen when you're building secure software. But all that is at the manufacturer elements, at the -- and improving those elements. And we don't want to

begin putting constrictions on and lose any of that because we now have this new constraint of repair.

DR. MCGRAW: I see your point. I don't think we have to, but I see your point. So let's have the market figure that out. But the problem is that if we're marketing these things -- they used to be marketed towards tiny, so small was the new big, and then skinny. Now, skinny is the new big, but big is the new small. I don't know. It's very confusing. But, apparently, it changes battery shape, right?

DR. CRANE: Right.

DR. MCGRAW: And people want the thing, because -- I don't know. What's Apple's marketing budget again? Is it little? I think it's not little.

MS. GORDON-BYRNE: It's bigger than mine.

DR. MCGRAW: I'm an Apple shareholder, so that's cool. But, I mean, the thing is a lot of these consumer wants and desires are driven by advertising and they're just a coolness factor. They're not driven by security or anything else. And many of the factors are invisible to consumers.

Who said, in the first panel, nobody knows whether something can be repaired when they buy it at the store? Was it your mouse we were talking about? You bought a Logitech mouse? What the hell.

(Laughter.)

DR. MCGRAW: I thought you were a geek. Sorry, that's Paul over there.

So the problem is that these things like repairability and security are invisible to consumers. And the claims that are made -- well, there aren't any claims made. So maybe we should fix that so that people can make a more informed choice when they buy stuff.

MS. TODARO: George, I just want to have a followup question to that. Do you agree that the design decisions are not made for security or safety reasons?

DR. MCGRAW: What?

MS. TODARO: I think on -- for George, I'm sorry.

On the earlier panel, we heard that design decisions are often just made in response to consumer demand. And there was some discussion about it. He says to keep the devices together. So I'm wondering what your thoughts are on whether or not certain design decisions are made specifically with regard to the safety of the lithium batteries.

MR. KERCHNER: Oh, absolutely. And, again, characterizing the design choices and repair policies

as repair restrictions, I think, is incorrect. I mean, again, our members manufacture the safest batteries in the world, right? And our members manufacture the safest products in the world. And that battery manufacturer works very closely with that product manufacturer. And that product manufacturer goes to visit that battery manufacturing facility to make sure they're designing and manufacturing the safest batteries in the world.

And, again, that relationship between the product manufacturer and the battery manufacturer to manufacture a product that the consumer wants, whether it's a thin -- you know, as Gary said, a thin phone, that's the direction those manufacturers or products are going to go. If the industry or the consumer wants those thin products, those are the products our members are going to manufacture. But, again, for our members, it all goes back to making sure it's the safest product they can put in the marketplace.

DR. CRANE: Christine, can I address that, too?

So I need to recharacterize, also, the way you stated that. You said, are design decisions not made for security and safety. And I think it's the complete opposite, where there is this challenge of

this assumed element of the restriction component of this panel. Because I want to bring up what Gary just shared, is it would be great if we could get people to make consumer-based buying choices because of the security of the device or the repairability of the device, in addition to the features of the device and all those -- those are design functions. But saying that a product is designed without any of those considerations -- it doesn't magically show up on the market.

Take, for example, like I mentioned during my opening remarks, the improvements over the past decade in security so that we're able to take what was just a consumer device that we would never let into the enterprise -- that's where BlackBerry was. That was the domain of -- you had enterprise-focused technology and consumer-focused technology. And, now, you've got the smartphones that are the same device both in the consumer space and in the enterprise space.

DR. MCGRAW: In between, what caused that was this thing called the internet.

DR. CRANE: And all the other great features of it.

DR. MCGRAW: I'm totally serious. That

changed everything. So the idea of going, well, there was some enterprise stuff and then there was the consumer stuff, and the consumer stuff was better, well, they adopted the internet.

DR. CRANE: Well, it was the demand that drew it in, right?

DR. MCGRAW: Yeah.

DR. CRANE: So my point being that it wasn't done without consideration of security. It was done because consumer choice came in. And enterprise buyers are consumers, too, when you have a dual-use device like the ones we're talking about.

MS. GORDON-BYRNE: Okay. I just kind of want to see if we can pull ourselves back from batteries and talk a little bit more generally about repair. Because batteries are really a consumable, and they are -- they determine the lifetime of a product if they are not replaceable. And I think the battery industry could do a heck of a lot better job, or at least the designers of products could do a heck of a lot better job, selecting batteries that are safer to replace.

So we're not saying you can't design things that are unsafe, which is apparently common. And it would be nice to know if they are safe. But for

goodness sake, at least make them safe enough to remove and replace, because that determines whether or not a $1,000 product is at end of life in 18 months or a $600 -- or it doesn't really matter, but as soon as you insert something that has a finite lifetime into a product, that is the end of the product.

So I don't see batteries as being a problem for repair. I think it's a design problem. And if federal agencies want to get involved and say, we don't want to have batteries in our consumer products that don't do X, Y, and Z, fine. That doesn't alter the need for repair.

Same thing with security. I have yet to see an argument that says that if you open this product and you replace a memory card with another memory card, particularly if the memory card is the same brand as the memory card, that creates a cybersecurity risk for anybody. So I want to live in the world of the practical. I'm dealing with things like refrigerators that have password protection on parts for no reason other than to require a service call.

Example, refrigerator has a bad digital thermostat. Customer who's a friend of mine, smart enough, figured out what the part was, ordered the part. Part shows up, puts it in. It says, input

password. Calls up GE. They said, we can't give you the password, you have to have a service tech come out and input the password.

That's the kind of stuff that's thwarting repair. And I don't think anybody here is seriously thinking that's a problem of batteries or a problem of cybersecurity. That is a problem of the manufacturer trying to monopolize repair because maybe they want the repair revenue or maybe they want the dealerships to have a supporting revenue base so that they can stay in business. But whatever it is, it's not security and it's not safety. It is money. And we have to work on that.

(Applause.)

MS. TODARO: Gay, do you have any evidence that supports the argument that repairs done by OEMs or authorized repair centers are a profit center of any kind?

MS. GORDON-BYRNE: Oh, absolutely. I used to work for OEMS. Our average profit margin on an enterprise repair was 95 percent, which meant that if a competitor were to come in and say, I could do 50 percent off, the customer was like, wow, how can you possibly do that? And everybody in the back is going [snickering]. Of course.

The cost of parts is negligible. It's all cost of labor. And if you can have competition for repair, just like you do with cars, a manufacturer's labor rate could be $800 an hour, as was -- Tufts University told us.

DR. MCGRAW: By the way, that's beginning to change now. I have one of those new cars that has more computers than car parts, and getting that thing repaired is a pain in the ass.

MS. GORDON-BYRNE: Yeah.

DR. MCGRAW: We tried to get a windshield replaced. Nope.

MS. GORDON-BYRNE: Yeah. So there's a lot of -- competition will make everything better. You'll either get better service, better availability, possibly lower costs, not necessarily. Cost is just one of many elements. But, right now, we're being blocked from having any of those choices as consumers and we're being told we're going to hurt the manufacturer.

We're not hurting the manufacturer, folks, when we repair our stuff. It's our stuff. We bought it. They've already been paid for all of their IP. They've been paid for all of their R&D. Their investors have been rewarded or not. And there's no

reason that they have to then monopolize repair in order to get more money, because that's a tying agreement, which we're not supposed to have.

So let's get away from this whole battery thing and this whole security thing and focus on things have to get fixed. And we can't fix them now because we're being told we can't buy the parts, we can't buy the tools, we can't get the diagnostics, we can't get the manuals, and, oh, by the way, we're going to sell you things that are unsafe and they're going to blow up, and, therefore, you shouldn't be allowed to fix them. I find this absolutely ludicrous.

The cure for unsafe products is more repair. The cure for getting rid of faulty parts is more repair, not less. If you have something -- like the famous Samsung exploding Galaxy, they designed that battery with such poor tolerance it went off in flames by itself. Had they made that battery designed so that the battery was replaceable, it wouldn't have been a $7 billion loss. They would have recalled the batteries, popped in the new batteries. Things would have been fine. It's just the money. It's just the money.

MS. TODARO: Dr. Crane, do you agree that

there are certain types of repairs that could be made without compromising a product's security?

DR. CRANE: Well, yeah, I think we already covered that. But since you've given me the mic, I need to say here, I'm a security guy, so I don't understand --

DR. MCGRAW: I also have a mic, so I'm a better security guy that can use my mic.

(Laughter.)

DR. CRANE: Yeah, but I spoke first.

So I do not want to dismiss security or safety from this conversation. And it's important to keep it part of it. I'm excited that we're able to have a conversation about security outside of our little nerd world of security wonks. So please don't dismiss it.

MS. GORDON-BYRNE: How about an example?

DR. CRANE: It's important.

MS. GORDON-BYRNE: How about an example on an iPhone? How does a consumer -- how does Theresa repairing an iPhone create a security problem?

DR. CRANE: So you actually led to that when you said if you open a product and you change the memory card and it's the same model memory card, how does that cause an issue? And the issue, while you've

got one instance there, which -- ignoring the fact that you would have to validate if that really was the same model memory card --

MS. GORDON-BYRNE: Let's say you bought it from Apple.

DR. CRANE: -- and not just one where they had scratched off, because I had to deal with this before with counterfeit.

MS. GORDON-BYRNE: No, but let's say you knew --

DR. CRANE: Hold on. Let me finish. Where you had to scratch off the manufacturer and you write in a new manufacturer. Now, you're dealing with counterfeit parts. I mean, I had to deal with these before. And so you have to then do validation and testing and verify that this really -- you know, because there might be a serial number embedded in the silicon to be able to get to that level. So all that is a higher level of due diligence that needs to happen during the repair process to get it back to the point where there actually was a concern.

And if you don't do all that, if you just have to go with whatever part you can get your hand on, you're putting an unknown into your trusted environment. And that's where the security issue

shows up.

MS. GORDON-BYRNE: So if the product has a part replaced and it executes all the manufactured diagnostics, what's wrong?

DR. CRANE: I think I just covered that, right?

MS. GORDON-BYRNE: No, if the part isn't an authentic part and it still works fine and it executes all the manufactured diagnostics, what's wrong?

DR. CRANE: Because when you -- we've all taken our car in before and had them run a diagnostic and they can't find the noise while it's in the shop. So you have to drive it down the road and, all of a sudden, the problem comes back and you bring it back.

MS. GORDON-BYRNE: We're just talking electronics right here.

DR. CRANE: Just because it runs the diagnostic at that point doesn't mean that something else doesn't happen later with a failure or something else.

MS. GORDON-BYRNE: Okay. So the standard for the billions and billions of dollars that have been traded in used equipment around the world since the beginning of the computer industry has always been it runs manufacturer's diagnostics. If you buy a $10

million IBM mainframe in London and you ship it here and you turn it on and it runs IBM diagnostics, IBM puts it on maintenance, perfectly good product, what's different? If it runs diagnostics, it runs diagnostics.

DR. CRANE: Are you running it continuously?

MS. GORDON-BYRNE: No. There's a whole process in repair --

DR. CRANE: Are you continuously monitoring to make sure that the device is still operating with the same security parameters, that the certificate hasn't been compromised?

MS. GORDON-BYRNE: But this is hardware.

DR. CRANE: I mean, in security, we do it all the time.

MS. TODARO: This is not a security certificate.

DR. CRANE: It's continuous monitoring. We continuously --

MS. GORDON-BYRNE: Okay, but that's software.

DR. CRANE: -- monitor for security requirements.

MS. GORDON-BYRNE: But that's software. We're talking about a hardware repair, a defined,

discrete event.

DR. CRANE: No, it's because software embeds in the hardware -- software embeds in hardware. So we're always looking to see if a certificate has been recalled because it's been compromised.

DR. MCGRAW: Wait, is that kind of like --

MS. GORDON-BYRNE: Hold on, this is crazy.

DR. MCGRAW: Is that kind of like pancake mix has flour in it, so if you're the flour seller, you should own the pancake mix market?

DR. CRANE: No.

DR. MCGRAW: Okay.

DR. CRANE: Yeah.

MS. GORDON-BYRNE: All right.

DR. MCGRAW: That's the monopoly market.

MS. GORDON-BYRNE: I'm finding this insane.

MS. TODARO: Excuse my ignorance, but if there are certain repairs that can be made that don't compromise security, but those don't necessarily -- those aren't necessarily hardware repairs, what types of repairs could be made that wouldn't compromise security?

DR. CRANE: Now we're getting to some great -- where there needs to be some more security research done.

DR. MCGRAW: The answer is it depends on the design. And if we allow the people who control those design decisions to also control the right to repair, then we have the wrong people controlling all of the variables.

(Applause.)

MR. KERCHNER: You've got a lot of fans here, don't you?

DR. MCGRAW: Yeah, I hired them. You should see Twitter, man.

MS. GORDON-BYRNE: I'm not good at keeping my temper.

MS. TODARO: We talked a little bit earlier about consumers making a choice at the time of purchase, whether or not they're aware of the fact that a product would be particularly repairable. What type of information would consumers need to have at the time of purchase? And is anyone on the panel aware of specific products currently that do make that information available?

DR. MCGRAW: I think you can start it out the other way, like can't be repaired. If it can't be repaired, it should say, can't be repaired. And then we'll do the other thing later.

MS. TODARO: But would it be certain aspects

of the product couldn't be repaired? I mean, are there limits on --

DR. MCGRAW: There are certain products now that my --

MS. TODARO: -- the disclosures that would need to be --

DR. MCGRAW: -- understanding is they can't be repaired, like the whole damn thing. So can't be repaired. Just if the whole thing can't be repaired, you have to say so. And then we'll see if that gets us anything. Yeah.

MS. GORDON-BYRNE: Chances are that if it's been manufactured and it's not glued together, it can be repaired. It's a question of access to parts and also time. Because you can repair a lot of things that nobody wants you to repair if you're diligent and you have a multimeter and an oscilloscope and a whole lot of time on your hands. You can figure it out. But it doesn't -- consumers wouldn't do that.

DR. MCGRAW: I mean, security's always had the same problem. It's a really good question and no one knows what the answer is. Because you see things like military grade cryptography.

DR. CRANE: Right.

DR. MCGRAW: To this day, I don't even know

what the hell that means. That is a meaningless statement. But some people think that that's a requirement and they even put it in the procurement stuff.

DR. CRANE: It goes back to marketing. So I do want to share, though, I like it from the snark side of it, but I do want to highlight the Government has put out good security standards from NIST and NSA and some of the crypto standards that they've had. And the more that we can have manufacturers follow that -- and the good ones do -- to build better security into their devices based on those open standards and security patterns, it helps protect all of us.

DR. MCGRAW: Here, here. Excellent. But that's not a government mandate.

DR. CRANE: No, that is not a government mandate.

DR. MCGRAW: Just to be clear, it's really not.

DR. CRANE: Or legislation. It is voluntary to adopt those, absolutely right.

MS. TODARO: Gay, are you aware of any evidence that consumers research the repairability of devices at the time of purchase?

MS. GORDON-BYRNE: I think you might want to ask Kyle Wiens in the next panel about that, because he does rate products for repairability on his website.

MS. TODARO: And a followup to that question. We've heard anecdotally that consumers may care about this issue. Do you have any research that suggests that consumers do care about the repairability at the time of purchase?

MS. GORDON-BYRNE: Yes, and the answer is is that when we started asking consumers to write their legislators in support of right to repair, we've had over 80,000 of them write their legislators in support of right to repair, and only in those states where we've actually had bills moving. So in New York, it's over 30,000. And they write letters. They write whole letters saying, I can't fix this and I couldn't fix that, and my mother is this. They're very poignant. Consumers really do want to fix their stuff.

But I can't tell you that we had any kind of non-response survey, because we didn't approach it that way.

MS. TODARO: Is there any way for a consumer who brings their product to a third-party repair shop

to know whether or not that third party -- to vet that third party, I guess, to know if they have the expertise to fix a particular device?

MS. GORDON-BYRNE: There's no formal way. It's exactly the same process you'd go through in hiring a plumber or an electrician or a car repair guy or a babysitter. You look for reviews. You ask for recommendations. You know, there's so many online review sites now, it's hard to say that consumers don't have those tools. But in most states, there's no legislation -- there's no licensing process. There's no certification process.

All your certifications are either industry certifications that are created by the manufacturer as a testing program for their employees or their extended programs, or they may be some of these low-level certifications that kids get in high school, like the CompTIA A+ certification. There's no national one way to do any of this stuff. So it does fall on the consumer to use their own due diligence.

MS. TODARO: Did you have a thought?

MR. KERCHNER: Yeah. I mean, it's a great question. But, again, that's the reason why our members have these authorized repair facilities. The consumer knows that if they're at the authorized

facility, the employees in there, the engineers, the technicians or whatever have been trained on how to properly repair that $500,000, $2,000 device that the consumer wants repaired. So, again, that's the benefit of those authorized repair facilities.

DR. MCGRAW: So when cars become electric, because I think that's happening, are there going to be only authorized car repair dealers because of the battery?

MR. KERCHNER: Well, there are specific garages now, absolutely, that can only repair that battery if that's what needs to be repaired, certainly.

DR. MCGRAW: What about the rest of it?

MR. KERCHNER: What about the rest of it?

DR. MCGRAW: That was the question. If you don't have a battery problem, but you have a car problem in your electric car --

MR. KERCHNER: So again--

DR. MCGRAW: -- isn't it too dangerous to --

MR. KERCHNER: So if I have a General Motors Volt or a Bolt, whatever, I'm going to go into a GM garage that has that ability to repair that particular product, whether it's the battery or whether it's the electronics in that car that helps operate -- that

connects with that battery.

DR. MCGRAW: So all the car guys are SOL?

MR. KERCHNER: Well, no. I mean, if they get the proper training, they're going to be able to fix those cars, just like they have over all these years. All those guys that work in those garages for the last --

DR. MCGRAW: Not the ones who work for whatever, Corporation X, the ones who repair cars, like say in Vermont.

MR. KERCHNER: What's the question?

DR. MCGRAW: They're SOL? Is that right?

MR. KERCHNER: The guys in the garages?

DR. MCGRAW: Yeah.

MR. KERCHNER: Well, if they have the proper training, they can certainly fix the cars, certainly.

DR. MCGRAW: Well, if they get the parts, right?

MR. KERCHNER: At, again, authorized service centers.

DR. MCGRAW: The prosecution rests.

MS. TODARO: Sounds like (inaudible)

(Laughter.)

MS. GORDON-BYRNE: The authorized network is a marketing advantage, absolutely, a marketing

advantage for the manufacturers. They are not going to suddenly go out of the repair business, by no means. Back before 2000, when repair was widely, widely competitive and available in the computer industry, the manufacturers, even with these huge discounts, were still getting 85 percent of the business.

So right to repair allows for competition. It doesn't guarantee anyone will win. It doesn't guarantee that a lousy repair shop will stay in business and it doesn't mean that a lousy dealership will stay in business. It just means opportunity.

MS. TODARO: We've talked about some of the security and safety risks associated with or potentially associated with third-party repair, but aren't those risks still present if you have an authorized repair provider making the --

MS. GORDON-BYRNE: Yeah, absolutely.

MS. TODARO: -- repairs?

MS. GORDON-BYRNE: If a product is made so that it's dangerous to repair, it's just as dangerous for an authorized tech to repair it as anybody else, which is why there's things called recalls. There's a lot of electronics that get recalled from time to time, primarily power supplies and power cords because

that's where the most risk is. Almost all of your electronics are transformed low voltage, and so it's very hard to actually hurt yourself once it's detached from live voltage.

So the necessity of -- HP recalled 6 million power cords not long ago and it wasn't because they wanted to. They had a flaw. And it wasn't a big deal. They just replaced all the power cords. It's not unusual for these things to happen. But they are called recalls.

MS. TODARO: George, you have any followup?

MR. KERCHNER: No.

MS. TODARO: In terms of connected devices, are the security risks greater when you have a connected device? And if so, can you elaborate? I guess this goes to Dr. Crane and Dr. McGraw.

DR. MCGRAW: You want to go first?

DR. CRANE: Sure.

MS. TODARO: Can you elaborate on that?

DR. CRANE: I don't have the cute quips that you always keep coming up with. Very clever.

DR. MCGRAW: That's okay. I'll sell you one.

DR. CRANE: I'll take it.

(Laughter.)

DR. MCGRAW: I just used it, though.

DR. CRANE: I'll take used ones. So today, it sucks, right? I mean, so really, we need to talk about today and then tomorrow. We have some manufacturers who have better security processes than others. And they're the ones that consumers really are drawn to. We then have a whole lot of manufacturers that aren't there because it costs money to do good security. We see that problem all the time with everything from flaws in IoT devices, invasions of privacy, botnet proliferation going through smart devices. But the risk is that as we adopt those smart devices into our lives more, security needs to come along with it.

And if security isn't built into the design process or if it's made as a trade-off so that we can have more open access to the device, that's something that's going to cause -- it could have an increased risk than if we weren't just to be able to hold better security, engineering, and design principles.

DR. MCGRAW: Yeah, I think that's exactly right. The problem is when you connect something to the internet, you connect it to -- it's just like putting it out there in the street. So stuff can arrive. It can be bad stuff. People can do bad

things. They can hit your thing with a hammer. They can do all sorts of bad things to your device because you put it on the internet.

But we're rushing to put a bunch of stuff on the internet. And as Earl said, sometimes people don't care about security, so they might just ship an IoT light bulb that has a username and password that are admin/admin and everybody knows. And all of a sudden, you get the Mirai botnet out of that.

So the challenge, though, is that once we're connected, maybe we can actually fix some of those security problems, too.

So back in the old days, we used to worry about patching software. But we've come to realize that we can't build perfect software, even if everybody reads my books, which I hope everybody does. The problem is that it's very hard to do, and so unanticipated things happen. The threat landscape changes. All the things you said about continuous monitoring are right on the money. The issue is we've got to be able to get to that device to fix it, to repair it, even if you're the manufacturer and you want to repair it. A patch is a repair that comes from the manufacturer of that software.

DR. CRANE: Yeah.

DR. MCGRAW: And so those mechanisms already need to be in place, in some sense, for software to be patched when we have internet connectivity. So internet connectivity is a double-edged sword. It's like a security disaster and it's also our only security hope.

DR. CRANE: Yeah. I would love to see the FTC -- rather than trying to look at issues kind of just like from a restriction standpoint, how could we encourage better security in our connected devices? And if we could start making it more aware so that consumers can make a more informed decision about security and giving them that choice would help all of us, especially as our neighbors all get internet-connected devices.

DR. MCGRAW: That's exactly right.

MS. GORDON-BYRNE: Yeah. One of the distortions we see in the repair marketplace -- and I think it's increasing -- is the number of manufacturers -- again, because repair has a very lucrative aspect -- is the increased number of links to getting the software patches and fixes that belong for security as a condition of allowing a hardware repair. So they've linked two pretty different things in terms of skill sets.

You've got a hardware tech like Theresa that's going to open stuff up and make physical repairs, but if she can't do that because there's some software certificate that she doesn't have or the user can't get, then the device isn't getting updated and the consumer's not getting a repair. So these things are blocking each other, too.

DR. MCGRAW: Yeah, so that's bad design.

DR. CRANE: That's bad design

MS. GORDON-BYRNE: I agree. It's totally --

DR. CRANE: That is not an issue of repair, though.

MS. GORDON-BYRNE: No.

DR. CRANE: That is an issue of the engineering and the market.

MS. GORDON-BYRNE: Yes, very much of the market.

DR. CRANE: I'm glad you brought this up, because kind of one of my favorite examples -- you would be surprised how many instances of Windows XP are still out there and still running critical systems, critical ICS systems.

DR. MCGRAW: ATMs.

DR. CRANE: Yeah.

MS. GORDON-BYRNE: COBOL.

DR. CRANE: I've got hacked into a few of those by the bank. So this is an issue that's not unique to repair. It's an issue that's unique to all of us needing to improve security so that we have -- so that we're able to build good software, deploy good software, and put security out there to be paramount. But the important takeaway is that that's not unique to repair -- I'm repeating myself -- not unique to repair and doesn't need to be driven by any legislation around repair. That gets really to having better security and putting security first in the marketplace.

MS. GORDON-BYRNE: We agree. Stunning.

MR. KERCHNER: First time.

MS. TODARO: A question from the audience about IoT devices. Dr. Crane and Dr. McGraw, do you think consumers should have access to internet off switches for connected devices in the event that there --

MR. KERCHNER: Run, Earl, run.

DR. CRANE: I was going to say I want you to --

MS. TODARO: In the event that there is a vulnerability or compromise.

DR. CRANE: I'll let you answer this one

first. Go ahead.

DR. MCGRAW: So if you have wireless at your house, you probably have an ISP. So here's a wire that comes in and you can unplug it. Internet off.

MS. GORDON-BYRNE: There you go. Good point.

DR. MCGRAW: So that. Is that what you mean? Who asked that?

DR. CRANE: Don't call them out. Don't call them out. I don't want them to -- you can talk to us afterwards. Happy to.

DR. MCGRAW: So the problem is that these Internet of Things devices are invading the consumer space. We used to do stuff like buy a light bulb and now we get a smart light bulb that you have an app. It takes, like, an hour and a half to get the light bulb to turn on. And you have to, like, watch a YouTube video of some kid, and you're like, oh, that's how. I just did that, really. It's totally ridiculous. And we expect them to be for normals, for normal people, not geeks like me.

DR. CRANE: How many security people does it take to screw in a light bulb?

DR. MCGRAW: Yeah. It's like way more than it used to. So that's a real challenge. And security

is not something that's kept in mind and neither is repairability. In fact, one of the biggest issues is just getting the damn thing to work at all out of the box. I'm serious about this.

I've played with a bunch of IoT things at a facility I've got, and it's just -- I'm glad I have a PhD in computer science and built computers for a few years, like you, and code. But that's not a consumer device really, yet.

DR. CRANE: So just to add a little bit more, there is no such thing as an internet off switch. You can't have an internet off switch. We're too connected. This was a question that came up all the time at the White House.

DR. MCGRAW: You can unplug at your house.

DR. CRANE: You can unplug at your house, but do that for a power grid, right? We had this discussion a lot at the White House when we were working on all of our national security policy elements and how can we help protect the nation. And every so often, the idea of an internet off switch would come up to say, well, if I unplug it, then no bad things can get to it, right?

But as we discussed earlier, we have to

continuously always be monitoring these devices and providing patches and updates and configuration. And the IoT devices aren't static. They are always dynamic and always changing. That's why they're internet-connected. And so what we need is to be able to have security built into that ecosystem, which is the core of what we've been pushing manufacturers to build into and improve. And anything that kind of stops that, I'd say, is a bad thing.

DR. MCGRAW: I'm not sure why we're talking about that.

MS. TODARO: I guess as a possible solution. So if a consumer experienced a vulnerability or a compromise because their device was repaired and compromised in some way, is there a way that they can just --

DR. MCGRAW: Throw it out.

MS. TODARO: -- disconnect?

DR. MCGRAW: Yeah, smash it.

MR. KERCHNER: Recycle it.

DR. CRANE: Right, recycle it.

DR. MCGRAW: Don't smash it. Not yet.

MS. GORDON-BYRNE: I disagree that the premise is that the repair caused the vulnerability.

DR. MCGRAW: Yeah, that's an interesting

premise.

MS. GORDON-BYRNE: I start not liking that premise because I don't see how it happens. I see software -- all of the networking, all of the internet connectivity is fundamentally software. There's very few things that are on the hardware platform that are -- in the consumer level -- I'm not talking enterprise -- that are going to create a vulnerability other than by accidentally downloading some lousy piece of software, which, again, is software. So I just don't agree with the premise.

MS. TODARO: Any followup?

MR. KERCHNER: Definitely not from me.

(Laughter.)

DR. MCGRAW: You can't download batteries yet.

MR. KERCHNER: No. Just wait.

DR. CRANE: They'll start beaming energy, wireless energy.

MR. KERCHNER: Wireless energy.

DR. MCGRAW: Yeah. Just don't stand between (inaudible).

MS. TODARO: One question that I want to ask on the physical safety of certain repairs is years ago cars were repaired by independent repair shops or by

individuals in their driveway --

MS. GORDON-BYRNE: They still are.

MS. TODARO: And they still are.

(Laughter.)

DR. MCGRAW: You don't drive, do you?

(Laughter.)

MS. TODARO: I certainly don't fix my car. So is the conversation shifting now because we think that products are more dangerous than cars have been or do we just think that certain products that are used in devices today are more dangerous so we need to take repair out of the hands of consumers and -- or an argument is made that we need to take the repair out of the hands of consumers or third parties?

MS. GORDON-BYRNE: I definitely want to speak to that because the safety question is raised constantly in legislative settings where various opponents come forward and say, oh, consumers are going to be unsafe. And I'm like, how can that -- if you're willing to drive a car and accept all the safety risks of driving, the idea that you could hurt yourself while repairing a non-line voltage product is pretty out there. Everything in your car is way more dangerous in use than it is any piece of electronics

in use or under repair.

So I regard that as a stall tactic or a "let's see if we can scare the legislators so they don't want to let anybody fix their stuff." And as soon as they realize that, oh, yeah, taking an alternator out of a car and putting it up on a hoist and dropping it on my foot is pretty dangerous, but it's a hell of a lot less dangerous to open up the back of a computer and put in a new motherboard or a new screen. So the relative danger I think it's very much of an excuse.

MS. TODARO: George?

MR. KERCHNER: Yeah. That one, I'll have to chime in on.

So I think your question is, are products more dangerous? I think the short answer to that is yes, absolutely. So I'm old enough, unfortunately, to remember when phones were powered by nickel cadmium batteries. Nickel cadmium, you know, no flammable electrolytes in there. They're not regulated as a hazardous material by the Department of Transportation. But as soon as that switch from nickel cadmium to lithium-ion, you now have a battery that has a flammable organic solvent in there. It's a regulated --

MS. GORDON-BYRNE: What about lead acid batteries?

MR. KERCHNER: It's a regulated hazardous material by the Department of Transportation international standards. And, yes, the short answer is it is a more dangerous product than 25 years ago when these phones were powered by nickel cadmium batteries.

DR. MCGRAW: Coming to cars soon.

MS. GORDON-BYRNE: They are in cars.

MR. KERCHNER: And you as a consumer have the choice of whether you want electric vehicle, hybrid electric vehicle, or that flammable gas-powered vehicle we've all been driving safely for, what, 100 years.

DR. MCGRAW: I want a horse.

DR. CRANE: They bite.

MS. TODARO: Well, I want to thank all of my panelists today. I think this was a very lively and informative discussion. So I very much appreciate it. So if everyone can give them a round of applause.

(Applause.)

MS. TODARO: We are now going to take a 15-minute break and we'll concluded with Panel 3.

Just as a reminder, the cafeteria is closed,

and if you leave the building, you'll have to go back through security. Thank you.

(Break.)

PANEL 3: WHAT'S THE FIX?

MR. SALSBURG: Could you please take your seats? We're going to get started in about a minute.

(Pause.)

MR. SALSBURG: Good afternoon and welcome back to Nixing the Fix, the FTC's workshop on manufacturers' repair restrictions.

I'm Dan Salsburg from the FTC's Office of Technology Research and Investigation. A reminder, please turn off your cell phones. Do not try to take out the batteries though here, apparently. We want to avoid that.

(Laughter.)

MR. SALSBURG: But if you could silence them in some other way, that would be great.

If you have questions, please write them on a card like this. The cards are available outside or from one of the FTC staff that are circulating. And you can just give it to the FTC staff if you have a question. And we will try to ask some of these. If not, I can assure you that the FTC staff reads all the questions that are submitted and they often are very helpful for us understanding the ideas that people have about what they're hearing.

So for our third and final panel of the day,

we'll be discussing possible industry and legislative approaches for ensuring consumer choice in repair markets. I am joined by Minnesota State Senator David Osmek to my left; on Skype, who you can see on the big screens here, Vermont State Senator Chris Pearson; Aaron Lowe, who is the senior vice president of regulatory and government affairs for the Auto Care Association; Sarah Faye Pierce, the director of government relations for the Association of Home Appliance Manufacturers; and Kyle Wiens, the co-founder of iFixit, the repair community known for open source repair manuals and product tear-downs.

We're going to start by having each of our panelists give a three-minute statement. I know this is a little bit less -- a little shorter time than our previous panelists, so hopefully you don't feel like you're being a little bit ripped off here. But we want to just have a brief statement and then get straight into the questioning and discussion.

MR. LOWE: Is there someone we can protest to?

MR. SALSBURG: You can submit a comment card and I assure you we'll read it.

State Senator David Osmek, would you like to begin?

STATE SENATOR OSMEK: Sure. And for politicians, limiting us to three minutes actually might be a good idea. So just to let you know, thank you folks for importing this wonderful warm weather. If you want to know what it feels like to be a snowman in June, I can tell you what it is right now. We are in the process of continuing to do our legislative research and working on legislative -- or legislatively digital right to repair or the fix-it laws.

We have gotten some traction. We have gotten some movement. I actually can read, for those who want to, the two paragraphs that actually are Minnesota's right to repair law. And as Gay sort of gently said no to, it really is very specific to, we just want to be treated equally. And I can read it if you're interested.

But I did come up with one solution, maybe. Of course, asking a government official for a solution might not be a good idea in this town because they don't come up with any of them, it seems like. However, for our friends in the FTC, why not create a repair score? And we put stickers and scores and everything on every piece of equipment. Go look at a pop can. You get to see what every chemical is you're

drinking.

Why not say, if you're manufacturing a digital piece or an electronic piece in the United States that you can -- you need to look at the top 20 repairable items that you have to do. And one of them for a cell phone would be battery replacement. Why don't you, say, take the top 20 issues that any electronic has and create a score that says, of that number, 70 percent or whatever the percent is repairable. So it's going to tell the consumer right away -- and I wish this thing would stop chirping at me. You can tell the consumer right away and they can make the decision on what they want in a device. If they want to have a repairable device, they will look for a high repairable score.

And then not only put on there, let's say, 70 percent is repairable, then you put another number, slash 20. Of that 70 percent, or of the repairable items, the top 20 repairable items, 20 percent of them are ones you can fix. So that will also tell the consumer, hey, you can repair a lot of stuff on this thing, so if it goes bad, but you can also fix a certain portion of it yourself. You know, let the consumers make a decision.

Minnesota has sent you a guy named Al

Franken and recently sent you somebody called Ilhan Omar, active Socialists as far as I'm concerned. If you look at my legislative career and you look at what people in my state say about me, I'm one of the most conservative people that you're going to find. Hard to believe Minnesota has any, but there are a few of us. But we actually believe in consumers making the choice, and I'll talk maybe more about that as we go along.

But for the Federal Trade Commission or some other enterprising congressman or senator in the room, which there aren't any, why not create a repairable score to let the consumer make the choice. And you know what's going to happen? You're going to drive people to the devices and drive the industry in the direction you're going without forcing them to do it by a legislative mandate. So thank you.

MR. SALSBURG: Thank you, Senator Osmek.

Let's turn to Senator Pearson from Vermont.

STATE SENATOR PEARSON: Well, thank you for having me on the panel engaging in this important consumer issue. And I share my colleague's thought that this is not a partisan issue. It brings together fun coalitions.

I was the original sponsor of the right to

repair bill in Vermont. From that discussion, we developed a task force which spent about six months in late 2018 exploring the issues you've been talking about today. Vermont may well make progress on this, but I would frankly rather see a federal answer. I think consumers everywhere in the country want and deserve these rights. And the industry deserves the certainty of one rule rather than a patchwork of solutions that we cobble together as states because we're trying to fill the void left by a lack of federal action.

Just personally, I've owned several iPhones. I've never opened one up, but I've watched skilled people do it. I've had screens replaced with original parts culled from other phones, iPhones, and I've had knockoff parts, and I can tell you there was a huge difference in quality. I also had my camera break once and, according to Apple, nobody in Vermont could fix it. They wanted me to send it to them. But in addition to being a legislator, I run a small consulting business from my phone. So sending them my phone for a week was like evicting me from my office. It was a non-starter.

In the end, I set up an appointment at an Apple store when I was traveling out of state, and it

was fixed in an hour. You know, the fact is, that's not a realistic option for most Vermonters. We don't have broad access to authorized repair. But Vermonters have a tradition of fixing things and, frankly, wearing them out.

And one of the interesting points we heard in our task force was, as I think you've heard today, over 90 percent of repairs to cell phones are screen replacements. We could certainly start there. The next most prevalent repair for smartphones is battery replacement. And I found it curious -- it was repeated today -- the Battery Association is very worried about giving access to authorized parts, saying it will be unsafe for consumers. But they ignore that today, we can get our batteries replaced. And so they are shutting shops out of having the proper battery and creating the very dynamic they tell us we should worry about.

Virtually all of the principles we talk about with smartphones apply to appliances like vacuums, refrigerators, TVs, on and on and on. In our task force, we were told by the Appliance Association appliances used to last 30 years. Now they last something like 13. It's, frankly, a problem when you have an $8 part break on your refrigerator and you

toss the whole thing out and go buy a new one for $1,200 because you can't get that part.

To me, the issue here is a balance between manufacturers' rights to innovate and sell products for profit and consumers and our ability to use products as we like. Right now, the equation completely tilts to manufacturers. The system hurts our pocketbooks. It curtails small local businesses. Meanwhile, we fill our recycling plants and landfills, while companies sell us more and more products with an ever-shorter lifespan.

The security and safety issues we heard earlier today were similar to what we heard during the task force. And to me, the arguments are largely bogus, and they fall apart. When we think about motor vehicles, I think we would all agree an automobile is one of the more dangerous products that we own and we control. To say that consumers should not be permitted to take electronics to a repair shop is basically insisting that our cars have to be repaired at the dealer.

We've rejected this argument as a society, and this has to do with a ton of steel that we're hurtling down the road, you know. We'd be wise to do the same when it comes to lightweight electronics,

heavy washing machines, everything in between.

I appreciate being here, and I look forward to our discussion today.

MR. SALSBURG: Thank you, Senator.

And, Aaron Lowe?

MR. LOWE: The Auto Care Association represents the independent aftermarket, so company -- we're vertically integrated. We represent companies that manufacture, distribute, retail, and install and repair -- install parts and repair vehicles.

So about 70 percent of car owners, after their warranty expire, go to the independent repair shops to get their work done because of price, convenience, trust. It's been that way since the invention of the car.

In a way, I feel kind of a little, I guess, embarrassed to talk. We have a right to repair law as has been discussed to some point. We had to fight really hard to get it. We started the battle in 2001 in Congress and fought really hard against the manufacturers and dealer networks to get it. We were finally successful in Massachusetts, but we had to go to a ballot measure. And if there is any question about consumer support for choice in repair, it was our ballot measure. It passed Massachusetts by an 86

percent to 14 percent margin. I mean, nothing passes by that margin in ballot measures or legislation.

So in that ballot measure, it required that the same tools, information, software that are made available to dealers have to be made available to the independent aftermarket at a fair and reasonable price. It also required -- and beginning last year -- required that all the manufacturers' proprietary tool software had to be maintained in the cloud and then available to an independent shop via subscription -- day, month, year -- to download onto a PC and then interact with the vehicle using a standardized interface.

So it was all to make it -- to provide more information, better capabilities to the independent shop because the thought was the better the information and tools they have, the better the repairs and better service they're going to provide to the car owner. And it's been hugely successful. There are issues, of course, but it's had a lot of good impacts.

But notwithstanding all the benefits to our industry and to consumers, I do want to emphasize that we are not without problems that we're facing. We're still seeing Magnuson-Moss as a big issue. We're

seeing owner's manuals, TSPs, we're seeing marketing literature put out by the vehicle manufacturers that really scare the motorist or inform the motorist that they have to get their car repaired in order to maintain their warranty.

We're seeing wireless technology take over more and more right now and restrictions on the onboard diagnostic port that are making the vehicle manufacturer more and more the gatekeeper of the data from the vehicle that we need to repair those cars. And then we're seeing more embedded software that's forcing people to only purchase parts from the vehicle manufacturer if they even can get those parts.

ADAS, Advanced Driver-Assist Systems, on vehicles, which we all see as a major safety benefit, are also raising the price of repair by a large amount. So that's another issue. And then we're seeing actions taken by manufacturers to limit the availability of parts in the collision industry. So we're seeing a lot of issues that are still facing our industry, and I'm not even talking about some of the problems that the heavy-duty market is facing in commercial vehicles, as well.

So I want to thank the FTC for holding this workshop. I think this has been a great workshop so

far. I know I've learned a lot. But I hope this isn't the end, and I hope that the FTC will use this as a beginning to talk about some of these really important issues impacting the repair industry.

MR. SALSBURG: Thank you, Aaron.

And, now, Sarah Faye Pierce?

MS. PIERCE: Thank you. Good afternoon, and thank you for the opportunity to provide comments regarding the broad availability of repair options for consumers and to specifically discuss what my work at the state level has made clear. Legislative action on so-called right to repair issues is not needed. Year after year, the states have retreated from moving any right to repair bill past the committee stage.

This fact was further documented by a 2018 Vermont task force that was created to study whether legislation in this area is needed. And the final report, which I have here, has unequivocally recommended against legislation. My comments today will further illustrate this conclusion.

I'd like to first start by saying that I'm not an expert on Magnuson-Moss. Our members are aware of the existence of federal and state obligations and take them seriously. Other than the need recently to respond to state legislative proposals, we do not have

discussions within AHAM about warranty terms or other customer service terms and conditions. Those issues are considered competitive, and we leave them to the companies to ascertain their own legal obligations.

If consumers choose to attempt to fix their own connected product or hand it over to someone else, that is their prerogative. That does not mean, however, that manufacturers should be forced to hand over proprietary information to anyone with a business license. And in the case of home appliance repair, repair technicians enter the private homes of consumers, which presents additional circumstances that should be given careful consideration.

Home appliance manufacturers are continuously innovating in order to make better and more functionally-convenient products for consumers. This includes ensuring that consumers have access to specially trained and certified repair technicians. The people who repair appliances across the United States are mostly the local independent mom-and-pop repair businesses in our cities and towns. In fact, 90 percent -- let me repeat that -- 90 percent of repair shops that affiliate with the members of AHAM operate businesses with 10 or fewer employees.

Furthermore, AHAM members identified over

19,000 authorized servicers, repairers that are available to consumers across the country. In addition, our data shows that manufacturers typically require technicians to have certifications in several areas, state certifications to handle products that use electricity and gas; the EPA 608 certification to handle refrigerant gases for servicing and disposal; background checks, as well as local service or company requirements.

Also, constant communication and followup with local servicers is common when service tickets are issued. And this would include the type of service performed, the condition of the appliance, replacement parts used, if applicable, and follow up to ensure that safety and quality standards have been met.

Today, there are more than 860 million appliances in use, largely without incident. And 93 percent of consumers believe home appliance manufacturers do a good job in providing safe and quality appliances. Safety is the top priority. Product safety, for instance.

Authorized servicers are directly trained and tools are provided to, number one, allow technicians to understand the systems included on

every model and, two, repair those products appropriately. Most appliance products are required by the National Electric Code, as well as other applicable building mechanical codes, to be listed or certified under applicable North American safety standards like UL for electrical products or CSA for gas products. These safety standards ensure a product and all of its components will operate in a safe and reliable manner.

An untrained and uncertified repair person may not understand how to properly repair the product to ensure it continues to meet or exceed the safety standards, particularly, a connected product, which then raises cybersecurity issues. All of this puts consumers in jeopardy. A product that once was safe could be rendered unsafe by an improper repair or unintentional use of a counterfeit part.

Property safety, appliance repairs, when not performed correctly, can be the cause of property damage, like fires and flooding. Insurance claims, as well as increases in homeowner's insurance and premiums, could result if the independent third parties improperly perform in-home repairs.

And, finally, consumer security, the nature of major appliance repairs requires that repair

technicians enter the homes of consumers. In-home safety and security is of paramount importance to appliance manufacturers. Manufacturers who certify technicians require extensive background checks, as well as drug screening and, as previously mentioned, technical and safety training. If manufacturers are required to make all their technical information public knowledge, they decrease their ability to address whether the technicians who are entering the homes of consumers have completed the necessary technical and safety security checks.

Thank you very much.

MR. SALSBURG: Thank you, Sarah Faye.

And, Kyle?

MR. WIENS: I thought I'd tell you my story. I went to Cal Poly to study computer science a few years ago, and I had worked as a Apple authorized repair technician at a little Mac shop. I remember I was making $6.50 an hour. And the iBook that I bought cost $1,849. So you can do the math and figure out how much time I had invested in that computer. And I was in the dorms, and I dropped it off the bed onto the power supply. And if I held the plug just right, I could get it to work. And I thought, okay, this is fine. I'm just going to Google how to fix this thing,

and then I'll be set.

And I was naive, and maybe still am, and assumed that because the information existed, it would be on Google, right. This is how this works. And so I Googled around for the service manual and I couldn't find it. And I did a little more research and I still couldn't find it. And so then I did maybe what any engineering student would do and I just started taking it apart. And eventually, I was able to find my way through, but it was rather frustrating. All it took was a little drop of solder on the cracked joint. I put it back together, and it was fine.

I did some more research, and my question was, why in the world was the service information not available because I had seen what the authorized world was like, and I knew what the service manual looked like. And it's just step by step, this is how you remove the thing. And I learned that there had actually been several people that had posted that service manual online, but that they had gotten DMCA copyright takedown complaints from Apple saying, we don't want you to share this information.

And since then, I learned that that's a trend across the board. You have medical device manufacturers sending takedown notices to biomedical

technicians at hospitals saying, do not share this information on how to fix this equipment. And there is a whole host of problems around people just not having access to this.

And I said, well, this is crazy. But I already know at least how to fix this one iBook because I took it apart. So I said, let me -- I'll take it apart again. And I'll take pictures and I'll put them online, and we've been doing it ever since. And, now, iFixit is the largest public repair manual ever. I think that Boeing may have some larger service manuals internally, but iFixit is rather large. We help over 10 million people a month learn how to fix things. I'm from California, and in the last 12 months, about 20 percent of Californians accessed iFixit to learn how to fix something. So clearly there is demand.

We had some questions in the last panel, is there demand? Are consumers interested in this? And the answer is overwhelmingly yes. We've had millions of people access iFixit instructions just on changing iPhone batteries. Apple has sold something like a billion iOS devices and they have 500 retail stores. Those stores cannot service the market. In the auto world, you said the independent supplies 70 percent of

the repairs. I think you're going to find that's the case overwhelmingly in lots of markets.

And as I step back and I say, what is the type of America that I want to live in, what's the type of society that we want to have, it's a society where we value repair. Right now, repair jobs are about 3 percent of American employment. Would the country be better if it was double that, if we were fixing things, if we had more jobs here at home?

If you look at manufacturing this, yes, we'd like to bring manufacturing back here. But it's only $4 or $5 in labor paid to an overseas worker to assemble this product, where Theresa is probably charging $40 to put a new battery in that phone and then happily employing people in her community.

So repair is something that at the aggregate level we need to be encouraging. And I applaud you for hosting this workshop and looking to systematically address and tackle these barriers. Because at a macro level, if we can solve some of these specific technical issues that are getting in the way of the repairs and a system working, we have a real opportunity, I think, to give the economy a shot in the arm.

MR. SALSBURG: Thanks, Kyle.

So let's turn back the clock to the mid-1970s. Some of you may not have been alive, so I'll tell you what it was like back then. I was quite young. But, apparently, at the time that Congress passed the Magnuson-Moss Warranty Act, there was a real concern over manufacturers tying their warranty coverage to the use of the repair processes of the manufacturer. And that led to the prohibition on untying that's in Mag-Moss.

So the first two panels today, we looked at how has the repair market changed and, really, does Magnuson-Moss do an effective job at protecting consumer choice in the repair market. We're going to turn our attention now to look at whether the law needs to be changed and, also, are there other things short of a law change that industry can do voluntarily. And let's begin by looking at industry initiatives.

Sarah Faye Pierce, you've explained that the repair market for home appliances is already really competitive. I think you mentioned that there are 19,000 home appliance repairers in the United States.

MS. PIERCE: Correct.

MS. SALSBURG: Can you tell us more about this market? Are repair shops typically -- they do it

for one manufacturer or are they authorized repairers for multiple ones?

MS. PIERCE: Sure, and perhaps we did have slides.

MR. SALSBURG: Do you want -- would you like to put your slides up?

MS. PIERCE: We were sitting down, and so I didn't grab the clicker. But if you could --

MR. SALSBURG: You can grab it now, if you'd like to just put your slides up if that would be helpful.

MS. PIERCE: Oh, yeah. I just thought we could flip it back a couple, but I'll just grab it really quick.

Okay, so here this slide depicts on the screen the availability of independent authorized repair technicians for home appliances in America. This represents the 19,000 number that I shared with you. There is a subset of those that are actually an in-network authorized repairer, which is distinguished from the independent mom-and-pops, right. So that only makes up about 20 percent of that 19,000. So we're looking at 17,000 independent small businesses that have an affiliation with our manufacturers.

And what those independents have the ability

to do is to go through a certification process with the manufacturer. And they have to take a number of steps, as I articulated in my opening remarks, to affiliate and then make sure that their technicians have the proper training and certifications to safely and properly conduct repairs on appliances.

MR. SALSBURG: So how expensive is it for an independent repair shop to get affiliated with a manufacturer?

MS. PIERCE: Price is a conversation we do not have at AHAM on any matter.

MR. SALSBURG: Okay. Senator Pearson, let me turn to you. Recently, Apple announced that it was expanding its authorized repair services to include every Best Buy in the country. Thinking about that and also this graphic that I don't know if you can see -- but the graphic that Sarah Faye Pierce put up, which shows lots of green dots all over America of repair shops -- is having authorized repair shops available for folks in Vermont, is that sufficient?

STATE SENATOR PEARSON: Well, I think that's a big part of the issue and some of where the interests of rural states really shines through. I mean, I would say my little story with the camera and my phone, Best Buy couldn't fix it. They were already

authorized. But, of course, most Vermonters are probably several hours from the nearest Best Buy. So it's only a part of it, whereas every mall in the state and around the country has a little kiosk there that will replace your battery, will replace the screen. It's a question of what parts they get.

You know, I wonder if I can just address, too, something that Sarah said about the task force which I was the co-chair of. And she suggested that we strongly recommended that we should not move forward. That is [broken audio] false. What we acknowledged was that the legislature, if they wanted to move forward, needed to recognize this was going to be a court challenge. It was abundantly clear -- every little meeting we had in a corner room in Montpelier, Vermont, folks from the industry came from [broken audio] the country to watch what we were doing in our little state.

So the fact is, the industry likes the profit center that [broken audio] and obsolescence gives them. They're not going to give this up without a major fight. And so as somebody who is helping the legislature understand the dynamics here in our report, we would say, you know, you've got to be conscious of this dynamic if you're moving forward.

So authorized repair is part of the solution. We need more, probably, although we heard earlier today that it is not so much a training as a business arrangement to favor some businesses over others. It doesn't necessarily signal skills. And so I think we're nibbling around the edges here, and I'd like to go back to the automobile parallel where it's up to me to decide if my neighborhood mechanic has the skills that I want to trust. It's not up to Honda or Ford.

MS. PIERCE: Dan, maybe I could just jump in there really quickly, and just to harken back to what the senator said about an affiliation rather than skills training, and that is not what we would call accurate for our technicians. Our technicians are handling refrigerant gases and, currently, we are in a process of transitioning away from the higher global-warming-potential refrigerant gases down to something that's much better for the environment.

Those gases are different and look different and operate differently in a product than the higher global-warming-potential. And we need to have technicians and service technicians who are working on these products who have the safety certifications, who also have the understanding and the training on how

those gases interact differently and which gases go into which products. And so it's very critically important.

STATE SENATOR PEARSON: But by that logic, our neighborhood mechanic shouldn't fix the air conditioning in your car, right? In many cases, it's the same coolant. I mean, over and over, we're going to hear these themes where, in fact, the reality is much more basic than the industry would like to have us believe.

We have skilled people that want to do the work. Are they going to be flawless? No. Will some of those businesses close because they're incompetent? Sure. But some of them will thrive. And the bottom line is I buy a product, I pay for it outright, I should be able to take it where I want to be looked at by whomever I choose.

MR. SALSBURG: So, Aaron Lowe, let's have you follow up on that, too.

MR. LOWE: Yeah. I mean, we don't have any problem if they want to have authorized repair shops. We have dealers in our industry, but the consumer makes the choice. They base it on trust. They base it on reputation. There's this feeling, almost, that the consumer is just too stupid to figure out where

they're going to get their car repaired, that there aren't resources out there to figure it out. Having an independent repair industry keeps everybody competitive, keeps everybody honest. It makes people better at what they do. It makes people better repairers.

You know, this whole issue of air conditioning fluids, I mean, refrigerant, we have to do the same thing in the independent industry. We have to train our technicians to work on the new air conditioning refrigerants that are out there, 1234yf. There are regulations that EPA has put out requiring individual technicians to pass certain certifications. So you have to do that by federal law anyway. So the fact that they're going to be -- air conditioning is -- you know, no independent could work on that, they have to do the same thing that an authorized shop would do in order to work on those refrigerants either in stationary or the independent part of the industry.

So, I mean, I think competition always seems to make a better world for the consumer and makes even the authorized people better at what they do. And to say that we're only going to allow authorization is really -- now you're just setting them up to become

-- to not provide those services at the best cost at the best level of service that they can.

STATE SENATOR OSMEK: Or what seems to happen is -- and I've run into this with a number of different constituents that have come to me -- is that they would like to take the training and they would like to have the authorization and they would like to be certified, but the manufacturer for that particular device or that particular item isn't currently training anyone and doesn't provide that as an option, that an independent person can take that certification.

And also, Ms. Pierce actually made a great point by just saying, well, we don't know what that cost is. I mean, if the manufacturer says, we'll tell you what we're going to do. We'll give you the training and we'll give you the -- if you pass the certification, well, that'll be $10,000, please. Well you can make it so cost prohibitive that the authorized dealer is the only one that can afford to be the one that can do the repairs.

And, really, we've got two different things happening here. We're talking about devices -- and actually, I really like that the home manufacturers are really doing the model that we want to do across

the rest of the industry, which is have more availability, as Mr. Lowe said, have more independence that drives competition, that drives innovation, that also drives pricing. And then you go to other items, which actually the previous panel talked about, which are just flat out software being loaded onto hardware that are poison pills.

So you've got many different issues going on here today, but I think we're talking through the same issues, that we need to have more of that competition.

MR. SALSBURG: Kyle Wiens, let's say the gasket on my refrigerator door breaks. What's wrong with me having to go to an authorized repair facility?

MR. WIENS: Well, the interesting thing with refrigerators is there has been a spate of manufacturing defects over the last couple of years with LG and Samsung refrigerators. And there's a class action suit going on right now. But all of my friends that are appliance repair technicians have just had the time of their lives the last couple of years because they have been working flat out doing nothing but changing out LG and Samsung compressors. And they are so busy, they don't have time to change

my gasket.

So from everything I hear, LG and Samsung have hired out every single authorized repair tech, and they're just so flat out swamped dealing with all these defects and the problem -- part of the reason that they're so busy is they go out to somebody's house, they install a compressor, three months later, they go out and they put in a new compressor in that refrigerator. Like they've got a fundamental manufacturing flaw and it's soaked up all of their repair capacity.

And that's the kind of thing that you would expect to happen. Like I'm sure that this is not planned obsolescence. I'm sure they weren't sitting there saying, ha ha, we're going to make these compressors fail in three months. It was a manufacturing mistake. I'm sure they're fixing it and that the next refrigerators won't have this problem. But, in the meantime, you need the free market to be able to absorb that. And that's where in the auto world, it's so healthy having manufacturers have maybe 24 percent of the market; the rest is independent. And that independent market can swell and absorb more impact.

If you look at what happened with the iPhone

battery situation a year ago, it came out in the press that Apple had been slowing down phones with older batteries. And, all of a sudden, everybody was like, wait a second, my phone has a battery? It wears out? Maybe I should get a new one. And so the whole world said, let me go into Apple and get a new battery for my phone. And Apple was booked out, and it was weeks and weeks and weeks to get an appointment at an Apple store.

And so I imagine your business did fairly well those couple months. Mine did as well, right? We had consumers installing kits themselves. We had repair markets. If it wasn't for the independent iPhone repairers, Apple would've been screwed. They would've never been able to make their way through the crisis. So this is where the economy as a whole is resilient. Any individual company's network is not.

MR. SALSBURG: So, Aaron, let's turn to an existing industry initiative. You were describing the MOU that the auto industry has. It came into being about five years ago, is that right?

MR. LOWE: Right, 2014.

MR. SALSBURG: And technology has changed in five years. If you could turn back the clock -- not to 1970, but to 2014 -- knowing what you do now, how

would the MOU look different?

MR. LOWE: Well, first of all, the MOU came about to save the patchwork of legislation that would have been created had we gone state by state to do right to repair. And so what we agreed to in the MOU is that we would enforce the Massachusetts law nationwide. All the manufacturers -- with the exception of Tesla, and we could do a whole day on Tesla -- signed the MOU. It's been successful.

However, there are issues, which I mentioned when I started, of the fact that telematics, or data that's transmitted wirelessly, was excluded from the MOU. Would we have liked to have had that in there? Yes, but this is pretty early in 2014.

And, right now, we're facing the issue of data starting to be transmitted by vehicles which we have no access to and which is now -- also with more of these parts of the onboard diagnostic system being locked out, we need access to that data wirelessly, both to compete with the dealers but also to perform a lot of repairs.

So we would have liked to have that included in it, but we are now working to revise the law in Massachusetts to include wireless data and to ensure that you cannot restrict access to the onboard

diagnostic system without doing it in a standardized way.

MR. SALSBURG: Kyle, do you --

MR. LOWE: In Massachusetts, I'm sorry.

MR. SALSBURG: And, Kyle, do you see any way to expand an MOU from auto care to all products? Is that conceivable or cognizable?

MR. WIENS: I think so. I think that's the direction that we need to go in. And it's a question of, you know, do you need the regulatory framework, can you do it in a voluntary fashion. I'm totally open-minded. It's been really interesting that over the course of -- you've had 20 different states introduce right to repair bills this year, there has not been discussion of a compromise at all. So I think maybe we need to get a little bit farther and set a baseline for kind of good practices on the part of the industry.

There was a great academic paper that analyzed the current situation with right to repair and saying, basically, where are we on a spectrum of repair freedom where you'd have a totally free, open repair market and you have a closed market. Cars are somewhere in the middle. They said the current situation with most products is that the default is

repair is not an option.

MR. LOWE: Can I just say one thing? I don't think we would have had the MOU at all unless we had gotten the law passed in Massachusetts. That served as the bedrock that then moved the negotiations forward because it was a fear of having a patchwork that really drove having the MOU and the realization that we needed to -- you know, a national solution was in everybody's best interest. We wouldn't have gotten to that step until we had gotten the law in one state that would have made that happen.

MR. SALSBURG: Let me ask this to Senator Pearson and Senator Osmek. Is that your modus operandi here, that you're assuming that if one of your states passes a right to repair law, then there will be some sort of MOU generally?

STATE SENATOR PEARSON: If you're looking at me, I mean, I think -- I serve in the state legislature, so I have modest influence on the Federal Government. I have more influence in my legislature, and we're trying to move this forward. That's one of the things that excites me about the conversation you're having today is, clearly, federal action would be better.

And I just want to point out, you know, we

were asking earlier in the day, do consumers want this. What was the vote result in Massachusetts? I think it was on the ballot a couple of times. Did it ever get less than 80 percent support?

MR. LOWE: It was only on one. It was only one time. It was 86 percent to 14 percent. There wasn't even a question.

STATE SENATOR PEARSON: I'd love to win my election by 86 percent. That is a pretty compelling result. I'd be curious what the senator from Minnesota thinks.

STATE SENATOR OSMEK: First, I agree with my colleague from Vermont. This shouldn't happen in the states. It really shouldn't. It's a federal issue. However, it seems to me, this place is dysfunctional as hell, and it's just not going to get done unless somebody pushes it.

And I've been working on this since I came to the legislature. I've worked on it every summer in bits and pieces and not gotten anywhere. And what's happened is is the -- one of the first times I finally got a manufacturer to show up -- they're represented by a piece of fruit; I won't say who they are -- and they sat in the back of the room, crossed their arms, and said no. That's all they did. They said no, no,

no.

Then you get John Deere. And I don't know if John Deere is in the room, but they said no, no, no. That's all they said.

Consumers are demanding this. Consumers are demanding this. You're talking to a conservative Republican from Minnesota who is locking arms with liberal environmental Democrats who hate putting things in the landfills any more than I do. I mean, I'm a conservative at heart. I don't want to fill up landfills. There's no reason for it. The first word of conservative is conserve. And it's moving down the tracks.

My suggestion to -- and I don't want to threaten people in the room that are in an industry -- but I just want to tell you, you need to come to the table and get something that works before it's too late because it may be just in Minnesota that it may happen. But if there's changes in Washington, it could be very ugly what could happen. Let's get something that works for businesses and works for consumers. That's what I want to do. And no is not the answer.

(Applause.)

MR. SALSBURG: So, Aaron, the auto industry

MOU generally worked because you have a discrete industry with parties that can negotiate an MOU. Is that correct?

MR. LOWE: Yeah, I think -- we have a broad industry in the aftermarket. So the two associations, us and the Coalition for Auto Repair Equality, negotiated the MOU with a broad -- with the Alliance and the Global Automakers.

MR. SALSBURG: And, Kyle, when you think of that, can you think of -- are there associations that represent every manufacturer and every repair shop? I mean, are there parties that could actually negotiate such an MOU?

MR. WIENS: Yeah. It's harder. I mean, the CTA who spoke earlier I think is the closest thing to an association. But even they're not comprehensive. I mean, it is a large fragmented industry. And this is something that I think is interesting. We've had conversations with folks inside a lot of these large electronics manufacturers that are arguing internally to support the legislation. What they're saying is, look, we're already doing a lot of this. The big brands are maybe the closest to complying. They have already this information they're providing to their authorized network. It wouldn't be very burdensome to

make it available to the public.

But then they look at a lot of the knockoff products that are flooding into the market from China, saying there's no regulatory floor for these folks. They can just glue something together, make it disposable, not make a service part supply chain. So that would be the concern is that -- let's say that you had the good actors at a large association sign an MOU, that they might be undercut by foreign competition.

I mean, it's interesting. So Vermont has one of the leading electronics recycling programs. And the regulators in Vermont are regularly going to Amazon and Walmart saying, hey, this tablet that you're selling on Amazon, they didn't register it with Vermont's recycling program, so you need to remove it from the market. And it's fascinating to see Vermont step up and take that kind of barrier to the market approach, which is necessary because you have to have a baseline. Before we start talking about repair, you've got to make some kind of recycling program available.

MR. SALSBURG: So let's stick with Vermont. Senator Pearson, why don't you -- we're going to shift now and talk about proposed legislation since we only

have about 15 minutes left in this session. You're, as you mentioned, the co-chair of the Vermont Right to Repair Task Force. You're the chief sponsor of the right to repair law there. Maybe you could tell us a little bit about what your task force did and what your takeaways were.

STATE SENATOR PEARSON: Well, by the end, we had a lot of the same conversations you're having today. We had industry folks in, telling us their side of the story. By the end, we [broken audio] looking at what other states have already done, laws on the books around warranty expansion in California. For instance, if you buy a product -- I think it's over $500 or over $100 -- you have the right to have that repaired -- it's a little bit different, but same wheelhouse -- for maybe it's five or seven years. You have similar laws in Rhode Island, in Indiana, New Hampshire.

So we started moving in that direction, recognizing that the discussion is going to take time before we really decide to welcome the court challenge that the industry would bring to us if we were to pass the straight-up right to repair bill. We decided to keep the discussion going forward and see if we could land where other states have landed and, in some

cases, had laws on the books for years.

It's my impression that those laws have not, frankly, been taken advantage of very much. People don't realize they have these rights. Repair shops may not realize it. But since the discussion has started anew, maybe there's more awareness events like today. You see it in the media. I notice when public radio covers my bill, I'm getting a lot of feedback.

There's something about this just kind of old-fashioned idea. I bought something, I should be able to fix it. I should take it to my uncle if he's knowledgeable or down the street to a repair shop if they are reputable. This is kind of an old-fashioned idea. To me, I see the political problem of trying to keep this going, trying to keep it in the limelight and see if we can't actually enhance the rights that consumers have and deserve.

MR. SALSBURG: Senator Osmek, about 20 states or so have introduced legislation on right to repair, including Minnesota. None have gone anywhere. Is that going to change? And if so, why?

STATE SENATOR OSMEK: Well, I would hope so. And I'm just going to read quickly what our requirements are in Minnesota. It's very straightforward. For digital equipment and parts for

equipment sold or used in Minnesota, the original equipment manufacturer must make available, on fair and reasonable terms, documentation, parts, and tools inclusive of any updates to information or embedded software to any independent repair provider or owner of a digital electronic equipment manufactured or on behalf of, sold by original equipment manufacturer for the purposes of diagnosis, maintenance, or repair. That's a long sentence. But that's really it.

Nothing in this section requires the original equipment manufacturer to make a part if the part is no longer available to the original equipment manufacturer. That's it. There's another section that basically repeats itself for security and locked and related devices. That's it. We just want to have independent folks available to get the same things that the certified ones do. It seems common sense to me.

We haven't gotten a lot of movement because, to be perfectly honest, I have some members in my own caucus that are more rural in nature and they do hear from tractor manufacturers. I'll tell you what -- and not so much the auto dealers, because you've already got your somewhat of a carve-out. I'll tell you what, if there is security or safety issues, I'm willing to

listen to what you want to have for a carve-out. I'm willing to include that in here. I do not want people creating unsafe conditions in a combine. I don't want an auger to turn on mysteriously and suck somebody into it. That's not going to be good on my campaign literature.

(Laughter.)

STATE SENATOR OSMEK: So, honestly, it's just something that we want to let people make changes to. An example -- I mean, I'm going to go to the server example. I went to OceanTech at Eden Prairie, very close to where I used to work, and they had piles of servers, piles of them, they were rehabbing from a Fortune 100 company. What they were doing is refurbishing them and reselling them to a school district in Alabama.

Everybody wins. The manufacturer wins because, guess what, if there's value in these servers that are not poison-pilled with software that can't be dealt with -- you already heard somewhat about that; if a company can get better value, rather than running it to the end of life, can renew it quicker before the end of life, sell it -- put it onto a resale market that goes to a school district that does not need top-of-the-line equipment, they save money. The

manufacturer gets a faster turnover. A small business in Minnesota makes money and has good jobs.

Who's losing? Who's losing? Who's fighting? And why would you fight this? That's what drives me nuts out of this whole thing. Why would you fight this situation because it just makes sense? That's the direction we're trying to go and that's why this legislation will be so common sense.

But let's get the people in the room and let's just not say no and solve some of these problems. Let's solve -- we had security guys. Let's solve the security issue. Put things behind firewalls. You want more in the legislation to punish people that are going in behind firewalls and going into encryptions and blowing things up and creating problems? We'll do that for you. But it just -- no is not the answer. We all benefit by this, not just by not throwing things away, but also being able to save them and recoup them. And that school district in Alabama, their taxpayers are happy.

So let's all win out of this situation and get some great jobs. And, actually, one of the -- it's real selfish. Minnesota is a hub for this activity right now. I'm selfish. I want Minnesota to be first because I want us to suck it all from Vermont

and New York all into Minnesota and have all those jobs there. Sorry, folks. I'm selfish.

MR. LOWE: Can I just make one point to --

STATE SENATOR PEARSON: Dan, can I jump in?

MR. SALSBURG: Hold on one second, Senator Pearson.

Aaron?

MR. LOWE: The average age of a car right now is 11.8 years, which continues to grow. One of the reasons is, of course, cars are being made better. But the other reason is that those cars are repairable and people of all income streams can have affordable transportation to do what they need to do. It keeps cars out of the landfill sooner. It allows cars to keep running. Now, it may not be great news for Detroit all the time, although they've been selling cars the last couple of years. But it is good for the motoring public. It's good for the environment. And it's been good for our industry as well, obviously.

MR. SALSBURG: Senator Pearson, do you want to comment on sending all Vermont's money to Minnesota?

STATE SENATOR OSMEK: Yes. He will. He will.

STATE SENATOR PEARSON: We actually have a

guy that's been helping me on the legislation who is a regional expert on iPhones. People in Albany and New England send the tough repairs to him. And he'll tell you [broken audio] diagnostics, for a $2 part he could save your iPhone that's dead. If he can't do it, you buy a new 8 or other iPhone.

But a funny thing -- I'm getting a bit of an echo. Can you guys hear me?

MR. SALSBURG: Yeah, we're getting a little echo, too, but we can hear you.

STATE SENATOR PEARSON: Okay. When I first introduced the bill, industry didn't come and ask for a little modification. They asked for carve-outs. And the industry that caught my eye was the medical manufacturers. And I thought, gee, you know, maybe we do want to take X-rays and MRIs and stuff and treat them differently. It's a little different than my laptop or my coffee maker. And I just had that thought privately. I didn't respond right away to the outreach from the industry.

The hospital up the street from me is a level one trauma center, a teaching hospital. The techs there sent me a letter and said, I'm so glad you're doing this. We are barred from repairing so much of the equipment in the hospital. It costs us

tons of money. We have the ability to do it, but we're not allowed to. It costs us money. It takes more time because we've got to wait for the authorized repair dealer to get there. And that really surprised me.

I mean, over and over -- we have the expertise in our rural parts of the country, in our urban parts of the country. The industry doesn't want us to make progress. It's not surprising to me that it takes time. They're enjoying the profits and having us buy new stuff at a highly frequent rate.

MR. SALSBURG: In the lead up to this workshop, we've heard from associations that represent manufacturers of a variety of industries and associations of repairs for a variety of industries, including medical devices. Have you thought about whether there should be carve-outs for other industries besides the medical devices, for instance, tractors, aircraft, home appliances, products with lithium-ion cells, or gaming systems and video games? Are folks coming to you, Senators, to try to get these sorts of carve-outs and have any of them convinced you?

STATE SENATOR PEARSON: They are all coming, and none of them have convinced me.

STATE SENATOR OSMEK: Well, I'll say that one of them did convince me. We did put a section into my bill that says nothing in this -- it says in section B, subsection 6, nothing in this section applies to medical equipment as defined by the United States Food and Drug Administration under the Federal Food, Drug and Cosmetic Act.

I do have concerns from a safety issue about somebody who doesn't have training and certification fixing something, and I'm having open heart surgery and, all of a sudden, they didn't fix it right and, now, I'm flat-lined. So I think there is a good reason. I also don't think they should be working on pacemakers. I think that's probably a bad idea.

But you know, we can talk through that, whether it makes sense or not. Maybe there's some things in a hospital that should be fixable by the custodial staff and there probably -- you know, I don't know. But let's talk through those. Up until this point in time, I haven't gotten that far. I've moved the ball to the 10-yard line, but I'm not getting very far.

MR. SALSBURG: So, Aaron, I'm not sure whether we can equate a pacemaker with a spare tire. But if I change my tire really incorrectly and forget

to put the lug nuts on, I can cause quite a lot of mayhem on the highway. Were arguments about safety and repairs made throughout the process leading up to the MOU?

MR. LOWE: The arguments for safety -- IPU is a big issue. There is a ton of issues very similar to what's been raised by the manufacturing industry in these device right to repair bills. But in the end, those didn't win out and we didn't put restrictions on right to repair. There were security issues that needed to be worked out. And so one of the things we did is we created a system called the -- I'm blanking out on what it is. But it allowed security codes to be monitored or tracked.

When a repair shop or an independent locksmith needed to replace a key or to re-energize a system that has a key code, we developed a system that allows a group to track that. So if there's a problem with it, we can monitor and law enforcement can take action. So we were able to address that issue, a special issue. And so the same things would come with any security issue, they would have to be developed. There are ways to address them and there are ways to allow for competition.

And so in the end, we passed the law. It's

been in effect. The world didn't end. Cars are being repaired safely and, you know, more and better information is out there. So I think -- you know, we heard the world was going to end. It didn't. It continues to be a very viable industry. And I think car owners can continue to trust their independent shops and technicians.

MR. WIENS: And one thing that I would note is that the law says the mission has to be available to consumers, and it is. If you go online, you can pay GM for information, for access to your car. It's not very much to get access for the day. And even the Korean manufacturers -- correct me if I'm wrong, but I think Hyundai and Kia went so far as just to make it available for free to everybody.

MR. LOWE: They did, but that was just really basic information. They did develop a site that was more for technicians.

MR. WIENS: Okay, got it.

MR. LOWE: We could talk about the Kia-Hyundai issue, but --

MR. WIENS: Sure, okay. But, I mean, fundamentally, this information has been made available to consumers for years, and it's been very successful and useful. And one thing I think is

really interesting -- we talk about safety. Well, let's get a baseline of information out there. If we're concerned about people doing repairs improperly, it seems like maybe the right reaction to that would be to train them better, not to withhold information.

I see this in the forklift world. All the forklift manufacturers make all their service manuals available very carefully. And it's their lawyers that are driving it because they know that if you repair a forklift improperly, you're going to have a problem. And so they see the way to mitigate their legal risk is, let's publish the exact precise right way to do it. And then if there is an improper repair, we can say, let's look at what they did. Let's look at the procedure we showed them on how to do it. And if they differed from the procedure, it's their fault.

Where if you put a system out there that it's complicated and challenging to work on and you withhold the information on how to safely work on it, maybe you're opening yourself up to some more liability.

MR. SALSBURG: Senator Osmek, one of the things that struck me when you were reading Minnesota's bill was what kinds of repairs it would cover. We've heard people argue that right to repair

would enable somebody to enhance products and modify them in a way that would be dangerous. Is there anything in what you read that would allow for modification that wasn't bringing something back to its original state?

STATE SENATOR OSMEK: True, there's nothing specifically written into the requirements that says thou shalt not enhance or make it better. It may be a byproduct of what happens. But then, again, why should I stand in the way of somebody knowing how to create a better -- creating a better mousetrap? I mean, if somebody figures it out, that's how innovation happens in the United States is somebody looks at it, looks at the manuals, figures it out, and says, I can enhance the usability of this product by 50 percent by doing this without breaking any law, without breaking the device, without breaking into the security of the device, without breaking into the intellectual property of the device. I mean, we already have enough intellectual property laws on the federal books and the state statutes to kill a horse.

So nothing stops it from happening. But, again, come to the -- the industries need to come to -- we've laid out -- the advocates here have very well laid out today all of our concerns. We've put

everything on the table. Industry needs to come to the table and work with us because if you don't, as I said a little earlier, it's not going to turn out well.

Because I know the other side and they're not going to listen to business guys like me that understand the issue and want to help make it a manageable situation. You're going to get something rammed down your throat. That's what will happen.

MR. SALSBURG: And we're going to end on that note.

(Laughter.)

MR. SALSBURG: So I'd like to --

STATE SENATOR OSMEK: Mister Positive.

MR. SALSBURG: I'd like to thank our panel.

(Applause.)

MS. SALSBURG: And I'm pleased to introduce for closing remarks Lois Greisman, who is the associate director of the Division of Marketing Practices.

CLOSING REMARKS

MS. GREISMAN: Thank you, Dan. Well, thanks to everyone. It's been quite an afternoon. I think it will come as no surprise to anyone in this room or anyone who's been listening on the webcast, people have different views about repair restrictions. And some of these views are fairly well entrenched.

What I'd like to do is just call out a couple of the points that were made today, the ones that at least stuck in my mind.

Repairs can cause harms to someone else and forcing repairability will drive costs and undermine security. On the other hand, we heard that security demands being able to fix things. The market's been characterized as one providing OEMs with a monopoly on repairs. At the same time, we heard that repair limits may have a negative impact on innovation. And some spoke at length about consumer demand for design as very relevant to repair limits.

Others indicated that safety concerns necessitated on who can do repairs. We also heard that repair limits are simply not realistic if you live in a rural area or if you just don't have access to authorized dealers. And there's an interesting lack of data on the quality of repairs by those who

are authorized to do the repairs versus independent repairers. And, of course, there was a robust debate over environmental issues.

So the good news, there were no thermal runaways.

(Laughter.)

MS. GREISMAN: And that's good. We came maybe a little bit close on some occasions, but nothing terribly worrisome. And all seemed to agree, at least, that it's not a question of whether devices should be repaired; it's a question of who can do the repairs. Are they the authorized repairers? Though, even with them, there's some debate whether that's a business relationship or a serious certification process. Should it be independent shops or should it be consumers themselves?

And then, as this panel discussed, there are some interesting issues concerning proposed legislation, the auto industry's MOU and whether that serves as a template that can be expanded to other -- if not all industries, some discrete segments of industries.

So you're all wondering, what next? Well, as Commissioner Wilson said this morning, this is what we do at the FTC. We do workshops. We do

conferences. We do roundtables to look at, probe, poke interesting issues that affect consumer welfare and competition hopefully to inform us at the agency so we can do our jobs better and also to stir public debate. And I think I can fairly say we stirred a little public debate today.

Research and comments on this are open until September 16. Please, there were gaps in information and research that were flagged today. Also, I'm sure there are some arguments that were made or issues that were framed that can be more fine-tuned, and that would be very helpful as we think about and consider what steps, if any next steps, we should take.

So again, my particular thanks to the panelists and for those who traveled to be here today. Also my thanks to all those who participated and watched via webcast and, of course, to the FTC staff who put this on. So give yourselves a big round of applause, and we are adjourned.

(Applause.)

(The workshop was concluded.)

CERTIFICATE OF TRANSCRIPTIONIST

I, Elizabeth M. Farrell, do hereby certify that the foregoing proceedings and/or conversations were transcribed by me via CD, videotape, audiotape or digital recording, and reduced to typewriting under my supervision; that I had no role in the recording of this material; and that it has been transcribed to the best of my ability given the quality and clarity of the recording media.

I further certify that I am neither counsel for, related to, nor employed by any of the parties to the action in which these proceedings were transcribed; and further, that I am not a relative or employee of any attorney or counsel employed by the parties hereto, nor financially or otherwise interested in the outcome of the action.

DATE: 6/17/2020

ELIZABETH M. FARRELL, CERT