FEDERAL TRADE COMMISSION

COMPETITION AND CONSUMER PROTECTION
IN THE 21ST CENTURY

Tuesday, December 11, 2018
10:10 a.m.

Federal Trade Commission
Constitution Center
400 7th Street, SW
Washington, D.C.

FEDERAL TRADE COMMISSION

I N D E X

WELCOME AND INTRODUCTORY REMARKS

MS. JILLSON: Good morning, and welcome to the FTC's hearing on data security. My name is Elisa Jillson. I'm in the FTC's Division of Privacy and Identity Protection in the Bureau of Consumer Protection.

Before we get started with the substantive portion of the day, I have a few announcements. First, please silence your cell phones and other devices. If you leave the building during the conference, you will have to go back through security, so please keep that in mind, especially during lunch.

If an emergency requires you to leave the conference center but remain in the building, please follow the instructions provided over the building's PA system. If an emergency requires an evacuation of the building, an alarm will sound. Everyone should leave the building in an orderly manner through the main 7th Street exit. You'll turn left and proceed across D Street to the FTC emergency assembly area. Remain in that area until instructed to return. If you notice any suspicious activity, please alert building security.

This event will be photographed, webcast, and recorded. By participating, you are agreeing that

your image and anything that you say or submit may be posted indefinitely at FTC.gov or on one of the Commission's publicly available social media sites.

Question cards are available in the hallway on the information tables immediately outside the conference room. Ryan Hsu and Mohamad Batal will be available to collect your question cards. Please raise your hand and they will collect your card.

For those of you participating via webcast, you can tweet your questions at FTC using the hashtag FTChearings. Please understand that we may not be able to get to all questions.

Restrooms are located in the hallway just outside of the auditorium.

And with all of that said, I would now like to introduce Andrew Smith, the Director of the Bureau of Consumer Protection at the FTC who will be making some opening remarks.

(Applause.)

OPENING REMARKS

MR. SMITH: Thank you, Elisa. So welcome to the FTC's hearing on data security. This is the ninth in a series of hearings that we're holding on Competition and Consumer Protection in the 21st Century. So thank you to all of the workshop participants for taking your time -- taking time from your busy schedules to share your expertise with us. Thank you for all of you for coming today.

I understand this is being livestreamed, so thank you to everybody in TV land. And a very special thanks to Elisa Jillson, Jim Trilling, and Jared Ho from our Bureau of Consumer Protection; Mike LeGower and Marc Luppino from our Bureau of Economics; and Dan Gilman and the many staff in the Office of Policy Planning that have made these two days possible.

So first a disclaimer. I speak only for myself and not for the Commission or for any individual Commissioner. Sometimes I'm not even sure that I speak for myself. That's because I'm new at this. I've been here about six months. And even more interestingly, all of our five commissioners are almost as new as I am. All have joined within the

last seven months.

So this is an excellent opportunity for us to revisit policies and question old assumptions. So I don't know with my disclaimer and my caveat about the amount of time that I've been here at the Commission, I really can't predict much, but I can predict this, that data security will continue to be an important priority for the FTC and that the FTC will not be retreating from its role as the nation's primary data security law enforcement agency.

Digital data security has never been more important to businesses and consumers. The rise of online banking, e-commerce, connected homes, connected cars, smartphones, and really with this, connected people, digital data security becomes more important every day. But hardly a day passes that we don't hear about a new security breach at a major company. And, of course, this morning is no exception.

By one count, there were more than 1,250 data breaches in the last year with 4.5 billion records compromised. There's an old saw in the data security business, I understand, that there are two kinds of companies, those that have been hacked and those that have been hacked but don't know it yet.

So what have we been doing for -- on data security? Well, like many things in government, we know we use the three-legged stool model. We have law enforcement, policy development, and consumer and business education. First and foremost, law enforcement. We like to think of ourselves as a law enforcement agency. That's where most of our work in this area is done. We have settled more than 60 data security cases on issues ranging from internet of things to children's data to financial records, and there's more to come. For example, in January, the FTC staff will be going to trial in D-Link, a case centered on IOT security.

Policy development. Two weeks ago, the Commissioners identified -- or the Commissioners, rather, testified before Congress about what data security tools the FTC is using and what additional tools it could use to protect consumers' data. The long and short of it was that the Commissioners testified in favor of data security legislation with APA rulemaking for the FTC, along with civil penalties and expanded jurisdiction over telecommunications carriers, nonprofits, and a couple of others.

So also in the realm of policy development,

we're currently undergoing a routine regulatory review of our GLBA Safeguards Rule, which is one of two rules that we have made and enforced with respect to data security, the other being the COPPA rule. When this rule was initially issued in 2002, it was revolutionary in that it was risk-based and prescribed a process rather than a standard or an outcome. It became a model for other risk-based state and federal laws, and also provided useful guidance on data security for large and small enterprises alike.

But in the fast-changing world of data security, very little stays up to date for 15 years, like the GLBA Safeguards Rule has. So we're in the process of revisiting that rule to determine if improvements are needed. Today's hearing is a part of the Commission's policy work, and the record developed today will help to inform the Commission further on how best to use its tools to promote appropriate data security.

The final leg of the stool is consumer and business education. So I brought along a prop. This is our Cybersecurity for Small Business publication. All of these materials are on our website, and that's FTC.gov/smallbusiness, and that's where most of the distribution of these materials is done. So these are

new materials intended for small businesses but really can be translated to any business.

It includes fact sheets. It includes videos on our website. It includes quizzes and similar training materials for small businesses. Included in here are sort of the basics of data security, physical security in the NIST framework. We also address four specific scams that target businesses, ransomware, phishing, email spoofing, tech support scams, and then we also delve into more technical issues such as vendor management, cyber insurance, both first-party coverage and third-party cover, email authentication, web hosting, and remote access.

So, importantly, this campaign is cobranded with NIST, DHS, and the Small Business Administration, and we also got input from the National Association of Insurance Commissioners. We held a series of roundtables with small businesses in 2017, and they all told us that they need a single unified message from the Federal Government. They were -- they felt as though they were getting different and sometimes conflicting messages from different government agencies and they wanted one single, unified message with easy-to-use resources about cyber threats and how to deal with them. So we responded with this new

business education campaign.

So that's a useful reminder that we're not the only ones policing data security and providing guidance. So you just heard about our critical partnership with NIST and DHS and SBA, but, of course, we also have the Department of Justice, the U.S. Postal Inspectors, and other federal and state criminal law enforcers who are on the beat. State and federal banking, healthcare, insurance, securities regulators also are policing data security and providing guidance.

And we have our good friends and partners, the state attorneys general and, of course, private industry initiatives, including the payment card network -- including the payment card industry data security standards, as well as standards promulgated by public utilities and the defense industry and others.

Yet despite all of our best efforts, we seem not yet to have achieved optimal data security. The daily rash of breach announcements make it seem as though all of our efforts are just a drop in the ocean. How do we explain this? On the one hand, maybe our current approach is working, and the apparent uptick in breaches is just a result of more

data moving online and the greater sophistication of attackers and -- or maybe more and better intrusion detection and reporting of breaches.

On the other hand, maybe our current approach to data security requires some serious rejiggering. Or maybe the current approach is solid, but we just need more of it and better tools to achieve it. So we're here today to ask tough questions about the state of data security and data security regulation.

What are the incentives to invest in data security, and are they enough? What does consumer demand for data security look like? Does consumer demand meaningfully drive data security investment? Should we expect consumers to participate in securing their own information? How can we best assess data security at specific firms and how can we communicate that assessment to the relevant stakeholders, to executives, boards, cyber insurers, card issuers, consumers, regulators? Which regulatory and enforcement approaches are working? Why are they working? Can they be improved?

And, finally, we need it take a hard look at the FTC. Are our tools up to the task of identifying and remedying lapses in data security? So we're going

to be examining these big questions over the course of the next two days.

This morning, we'll start by focusing on data breaches. Marc Spitler from Verizon Security Research will present on the Data Breach Investigations Report, the annual chronicle of data breaches and their causes.

Next, Sebastien Gay from Georgetown's Economics Department will describe his work on how some firms internalize the cost of data breaches and whether their stock prices take a hit and how those firms mitigate that potential impact.

And, finally, Al Pascual from Javelin Strategy and Research will describe some markers of how data breaches affect consumers.

This afternoon, we'll turn to two panel discussions. The first will discuss the incentives to invest in data security, ranging from consumer trust to compliance obligations to cyber insurance, and explore how companies make those investment decisions.

The second panel will explore consumer demand for security. During this discussion, we'll hear about emerging security ratings that allow consumers to compare the security of products and whether we can count on consumers to shop on security.

Tomorrow, we'll tackle data security assessments. Assessors from a variety of backgrounds -- big four accounting, security boutique, cyber insurance firms -- will react to a series of hypothetical assessment situations. In these hypos, panelists will address thorny issues, like who defines the appropriate scope of an assessment, how does a company with a tight budget and big problems gauge security, and when to look to inside expertise and when an outside perspective may be better.

Next, Commissioner Becca Slaughter and Joshua Corman, the Cofounder of the "I am the Cavalry" security initiative will talk about the current threat landscape and emerging threats.

Tomorrow afternoon, panelists will turn to policy with a pair of panels on the U.S. approach to data security and FTC data security enforcement. These panels will examine what regulatory approaches are working, what's falling short, and how the current approaches could be improved. So we have a lot to cover with presenters and panelists who have thought a lot about these important issues.

I'd like now to turn it over to Jared Ho in the Division of Privacy and Identity Protection and Marc Luppino in the Bureau of Economics, who will

start us off with a series of presentations about data breaches.

Thank you all for coming today and for helping us to think about the state of data security.

(Applause.)

PRESENTATIONS ON DATA BREACHES

MR. HO: Okay. Thank you, Andrew, for those remarks. And good morning, everyone. We're delighted to be here today to kick off the first session of the day. My name is Jared Ho. I'm an attorney with the Division of Privacy and Identity Protection at the Federal Trade Commission. My comoderator is Marc Luppino. He's an economist in our Bureau of Economics.

We will start out this morning with three presentations from our highly esteemed guests, discussing the current set of data breaches and the impact of those breaches on both firms and consumers. First, you will hear about the trends our experts are seeing. We will then have what we expect to be a lively conversation with our presenters who delve deeper into the perspectives on the threats to consumers' personal information.

We will be taking questions from the audience. If anyone in the audience has a question, there are question cards on the table located directly outside of the auditorium. Please flag down our conference staff, either Ryan or Mohamad, and they will be collecting those cards and passing them to us.

MR. LUPPINO: Okay. There are more detailed

bio online, but very briefly, we have Marc Spitler who leads the Verizon Security Research Team. He's a lead author of the Verizon Data Breach Investigations Report series and is involved in the development of the Vocabulary for Event Recording and Incident Sharing framework, otherwise known as VERIS.

We also have Sebastien Gay who teaches in the Department of Economics at Georgetown University. He specializes in financial privacy in real estate and economics research, and he’s an Assistant Director for Financial Analysis for the Congressional Budget Office.

And, finally, he have Al Pascual, who is a Senior Vice President for Research and Head of Fraud and Security at Javelin Strategy and Research.

With that said, I will turn it over to Marc Spitler for the first presentation of the morning.

2018 Data Breach Investigations Report

MR. SPITLER: Well, hello, everybody. My name, again, is Marc Spitler. I'm here to talk about the results that we found in the 2018 Verizon Data Breach Investigations Report.

A brief history for those of you who may not be as familiar with it. This is a publication that we put out annually. This was the 11th iteration of it.

So we've been doing this since about 2008 -- really about 2008-2009. And the reason that we started it in the first place was we just were not seeing enough real-world data being presented back out to the public on what is really happening as far as cyber crime.

There is a lot of discussions, and people that are selling various widgets and services about things that you need to be worried about and wouldn't it be awful if this happened. We had a lot of that type of information coming to us, but what we didn't really know is when people are actually suffering real-world data breaches, who's behind it, what are they doing, what methods are they using, who are they targeting, and why?

And so we put out the first report back then and we've started to grow it ever since. So we are -- obviously, me and my team are very, very fond of good data sources, and we were not wanting for data this year. As you can see from some of the numbers on the slide there, we had over 2,000 confirmed data breaches, and we had over 50,000 security incidents. And we defined a security incident as an event where either confidentiality, integrity, or availability of an asset was compromised.

So people could get a denial of service that

takes down their website. We would not call that a breach. We would call that a security incident. So just a really quick definition there.

And, you know, our corpus is now well over 16,000 breaches and over 3,000 -- excuse me, 300,000 security incidents. So really big, splashy numbers. I'm not trying to scare anybody with that. I'll try to reel it back in to kind of talk about how do we categorize these to be able to present something out to the public that they can actually take action on.

When we first started this out, we had a single data source. We've now grown that to over 60, so we have participants from law enforcement; certs, both domestic and international; cyber insurers; other forensic partners. So we have a pretty good diversity of data. This is not every single incident that happened last year, every single breach, so we don't answer questions like are we getting better or worse. What we're just trying to do is find, you know, what are the tactics that are being used, what does this mean to me if I'm in a particular industry? Do I have to look at something more often than somebody else? What's most likely going to affect me? What's my 3:00-in-the-morning call going to be?

And one of the things that we had to take a

look at is why are these happening to begin with. So when there's confirmed data breaches and it is malicious, what is the mode of the adversary? More often than not it's money. It makes sense. People are doing this not because they -- you know, it's not because of ideology very often.

It certainly can be for strategic advantage, which would be the cyber espionage attacks that we do see. But from a frequency standpoint, it's money. They're going after data that can be monetized in the form of personal information, payment card information, card information, banking information, and it’s to make a dollar in some form or fashion.

Now, this chart behind me is about breaches, and one of the more interesting trends is you don't actually have to have a confirmed data breach to make money anymore. One of the ways they do that is ransomware. Ransomware has actually been around for quite a while, but it's really started to get a lot of publicity in recent years, and our data actually backs that up.

So we are seeing within our data set an increase in ransomware year over year. It doubled last year, it doubled the year prior to that as far as number of incidents. So the little line graph behind

me tells a couple of interesting stories. The first one, what this is showing is what assets are affected. So ransomware, a really quick definition, it's malware that gets onto a system, and it will obfuscate or encrypt data and then reducing obviously the utility of said data and then the adversary will demand a ransom that you pay and you may or may not get a key to unlock that.

The first thing you might notice is that we actually have people on this slide. And you're probably saying, okay, how do you encrypt a human? You don't, but where we are able to figure out how malware got onto a system, if it involved some level of altering of human behavior via phishing, via email, we're able to note that.

It seemed to go down quite a bit. That's really more indicative of back in 2014 when we didn't have as many of these. We knew what the malware vector was. A lot of these cases we're getting now we know that ransomware occurred, we know what industry it affected, but they didn't provide us or they did not record how the malware got on there.

I would be absolutely willing to bet if we had knowledge of every single malware vector that people, because of the email being the means to get

in, would be much, much higher. Our data shows that email is the predominant means of getting malware onto networks. Not only does our incident data show that, but we have a contributor that detonates millions and millions and millions of pieces of malware per calendar year, and their data also shows that they're finding this data and they're detonating it and it's coming in via email.

So the one line that doesn't have as sharp of a drop but I think is very interesting and, you know, concerning is the one that says server. And it's kind of the second one there. And it's got a slow rise. And, remember, this is from a percentage of ransomware incidents, so the actually numbers in 2017, 2016, much, much higher. And when we see servers being affected by this, we realize that this isn't just one person, a user in your organization getting ransomware, having his or her laptop or workstation encrypted. That's bad. You know, no one wants that on a particular day.

What we're seeing is that foothold is not being used and encrypted straightaway. They're using that to move laterally within an organization. They're using it to find databases, file servers, even backup servers. Then they encrypt, and now you've got

a much, much higher criticality event that's happening. They're able to ask for a higher ransom, and there's probably a higher chance that someone's going to pay it because you're in a much, much worse situation than if it was just a single laptop.

And, so, ransomware is one of the things that we've have seen rise up over the last couple of years. That's why I have a slide here. And we have a section on it in the full report itself, so anything you see here is obviously going to be available in the full report and explained even more.

The next topic I want to kind of touch on is social engineering. So the human factor, I've already kind of alluded to it with how a lot of ransomware gets onto systems, but we have seen a significant amount of real-world data breaches begin with social engineering, notably phishing, but we're also seeing a rise in what we call financial pretexting.

Common examples of this are people in finance departments getting an email from -- and I'm using air quotes here -- the CEO that is saying, hey, you know, we need you to pay this invoice before you go home for the weekend. It has to happen now. Thanks for all your hard work. And they are duped into sending -- you know, basically wiring money

directly to the adversary.

Kind of like ransomware, there really wasn't a data breach there. You know, they didn't necessarily give them their banking information. They were just flat out tricked into sending money to the bad guy.

But we also see human resources departments actually being affected by this, too. And that ruse is I'm from a payroll company or you know, again, I'm an executive, and I need W-2 information for all the employees. So that is obviously a data disclosure. They're providing this W-2 information that's being used for tax fraud. Both of those kind of affect all industries fairly across the board. You know, anybody can be affected by that style of attack.

We also see social engineering phishing being used by a nation state or state-affiliated groups. It's how they're gaining their foothold. It's how they're getting that kind of a patient zero, if you will, within an organization to again move laterally within a network, move deeper to find ultimately their end goal.

As you can see, this slide is very busy. There's a lot of numbers on here, and we have a limited amount of time, so I will not be going through

each of these individually, but what this shows is a breakout of different industries and some of the styles of attacks that we see. And I'm focusing really on the top left grid there. So, you know, at the top, going vertically are some industries and going horizontally are some styles of attacks, like crimeware, which is financially motivated malware, typically opportunistic in nature, ransomware being a prime example of that. Cyber espionage, again, that's going to be all about motive, who the adversary is, you know, what they're after. Denial of service, pretty self-explanatory.

Some of these other ones are self-explanatory, but what you can focus on here really, really quickly is, hey, some of these cells are a dark shade of blue and have large numbers in them. You can even squint your eyes and be able to kind of understand this is a heat map. Some areas have a strong level of correlation between the type of attack the industries see versus others, so you know, a combination which would include restaurants, food service, hotels.

If you go down, you can see, wow, they have a very, very big problem with people attacking their point-of-sale environments. It makes a lot of sense.

They process a lot of credit cards. Cyber criminals enjoy credit cards because they can make money off of it, and we already saw that slide, which is what motivates most people, so we see a strong correlation there. So people can just take a look at this single figure.

And there's a lot going on here. I could tell two hours of stories on this, but you can begin to say, hey, am I going to spend my time and my resources on a problem that's affecting me at a high level of frequency? Am I putting my money in the right place, or am I focusing on something that maybe isn't going to be as important to me because of my industry and what has happened historically to people like me?

And, again, this is all in the full report, so you can absolutely review this, and you can draw a lot of interesting stories from it. Again, I'll touch on a couple of the tactics that are being used. We talked about ransomware. We talked about some of the social attacks, primarily phishing, which is, you know, via email, or what we call pretexting, which is really a little bit more sophisticated than just a phish, which is more of a fire and forget, spring and prey, if you will, type of tactic. Pretexting is

where you develop a dialogue. You actually have a story. You have maybe done some intelligence-gathering to know who the right target is within that organization, but some other things are happening, too. All right?

We see use of stolen credentials as one of the primary tactics that adversaries are using. When we think about hacking and when we think about the bad guys and you have maybe this Hollywood vision of someone, you know, in a dark room probably wearing a hoodie and they're, you know, hammering away at a keyboard and they finally find that way in, in reality what they're trying to do most often is to phish some credentials off of someone and then reuse those. Why would they want to do something harder than that? Why would they want to do something that could be detected easier than reuse of credentials?

So we see a lot of attacks on single-factor static authentication. And we see that used all too often to protect highly critical types of data where we need to have stronger authentication, not just from an outside in to your network, but also even when you're on your network. We need to see stronger barriers between that first laptop that might be infected and other areas with other deeper security

zones.

The other types of malware that we're seeing, we see what's called backdoor or command and control. That establishes that foothold, that's persistence and allows the attacker to take hold of a system and use that as their entry point, and they can issue commands to it. So you can kind of see -- if you took a look at some of these, you see phishing, which can lead to back doors and C2s, which can lead to other types of malware that will capture credentials, which can lead to the reuse of that. So you see how these things are not mutually exclusive, but they can go in order and tell the story about how attackers are really trying to go about their business.

So that's kind of a high level of the things that we are seeing. And certainly, we'll have time to go over this in more detail as we go along with the panel. In front of you is the URL for the full, 80-plus-page report. And, hopefully, you'll be able to take a look at that. And if you do have any other questions, you can -- that report will also have email addresses that you can actually come back and ask us questions about the data, and we'll be more than happy to answer those.

MR. LUPPINO: Thank you very much, Marc. We'll now turn it over to Sebastien Gay for the second presentation this morning.

Strategic News Bundling and Privacy Breach Disclosure

MR. GAY: Thank you. Marc, Jared, thank you for inviting me this morning to talk about my academic research on privacy breaches. I want to remind the panel and the audience that I'm here in my personal capacity. None of these views reflect the views of my current employer on this particular topic, and I do not have any ongoing research on the topic at the current time.

Marriott, Target, Yahoo, Home Depot, and Anthem, all of these firms were breached recently. After the breaches, most of these firms did not encounter large decreases in their stock price. Most of them actually had new highs within a week of a disclosure, so what could explain this?

A privacy breach is a short-term crisis for a company. With thoughtful preparation, like any other crisis, it can actually be prevented. Preparation requires prevention, so let’s avoid it from Marc. Loss mitigation, it happened, what's the bottom line, let's get the PR involved; brand management, so let's restore a firm's reputation; and

customer relationships, which is usually what you lose once you have that type of privacy breaches.

Remediation costs for firms that fail to adequately protect consumer data can be quite large. Costly lawsuits, payments for credit report monitorings and actually call centers, and loss of future businesses. In a well-functioning system, firms would protect themselves and insure themselves against those risks.

And, so, the paper right here was asking the most important question at the time, that was could firms leverage media coverage to protect themselves from costly privacy breaches. So in my paper that I think is available online, "Strategic News Bundling and Privacy Breach Disclosures," I examine how firms can build up a repository of positive news that could then be used at or around the same time that a privacy breach is disclosed to offset its negative effects on the price.

So privacy breaches, as established before by Marc, are unexpected and usually negative news for companies and the stock market. Given their unexpected nature, the effect of privacy breaches has been difficult to measure in the economic and finance literature. When using event studies to examine the

price of a stock of affected firms before and after the disclosure of a privacy breach, academic papers have found both a positive and a negative effect.

So the question here was, why could that be? And so, looking at the state in which the breach happened, you can look that there are discrepancies in the disclosure laws. The legal disclosure time for a privacy breach, depending on the state, can depend on like -- can be a few days to actually a few months. That potential lag raises the question of whether firms strategically releasing all the news around the same time as a privacy breach can attenuate the effect on its stock price and then provide a softer effect on its reputation and its brand name.

So now, let's get on to the data that was used in the paper. I have a list of privacy breaches that I compiled from 2005 to 2014. At the time, I relied a little bit on the Verizon report, but there was also no official reporting standard that was adopted. So a compilation of all privacy breaches ended up being a very difficult task.

Data validation was important, and I used more than four different sources to try to find out whether or not the date of a release was correct, when the breach actually happened, and the number of

customers that were affected by the breach, as well as the magnitude of the breach. The problem here is that the term like “breach accounts” is very vague and used a lot of times.

Stock prices and other data on companies are available through academic resources, and the news data came actually from a very rich data set that compiles all other news that are available for every company with a time stamp. So think about something like for the data set that I had, like 13 million observations.

The news data are classified into three types -- breaking news reports, news reports, and press releases. Overall, the paper contains 542 privacy breaches for the time period 2005 to 2014. It doesn't contain all of the incidents that Marc talked about because I had to match it with stock market data. And the panel, as I mentioned, had more than 13 million observations.

So during the research project, a few, like, patterns on the data emerged. The first one, very interesting, is that not all privacy breaches are reported in the news. And actually, 50 breaches that were available in the sample were not present at all in the news at any point in time. More than 30 to 50

percent, depending on the industry of the breaches, were not even the target of any, like, breaking news alert.

Two, there was a lag between the time of reporting and the actual breach that can be actually quite lengthy. It went from a few days to years, and we may want to talk about it with, like, the panel, but when the FBI gets involved and there's an investigation, we can -- the time at which you have to report your privacy breach can actually be extended.

The third one is firms are ready to announce a remedy most of the times when they disclose a privacy breach, so they come ready for it.

Fourth is only half of the privacy breaches in the sample reported an actual or even estimated number of records breached.

And fifth, the more scary one, is firms can actually be breached multiple times. Some people may say they don't learn. Some others may say, like Marc mentioned earlier, show me the money. It happens more often in the retail, finance, and insurance industry, so Social Security numbers and bank accounts are very, you know, valuable to hackers, so they may be more willing to go back to the same source.

So intuitively, privacy breaches reporting

and media coverage can actually be thought of as some sort of a tide. The paper establishes that there is a sharp drop, on average obviously, in the average daily negative news compared to the usual level right before firms are disclosing a privacy breach. And this result is all the more surprising that I'm including in that number the actual release of a privacy breach as a news event, so really, if you take that out, it's almost -- you would get into the negative, if you wanted to push that.

More surprisingly, there's also a decrease in the amount of positive news right before and a strong increase right after the disclosure of a privacy breach. So this pattern seems to suggest that there is an intentional timing of disclosure when firms release a privacy breach.

So the paper runs a series of modified event studies using the amount of abnormal news defined to make it simple as the deviation for the mean number of new stories on a given day. The idea behind it is a firm like Apple has more news on a given day than Colgate. So -- and I do that for both positive and negative abnormal news.

So what you notice is that there is a significant negative effect of a breach disclosure on

the stock price on the day and the day after the disclosure, so something like 24 to 27 basis points. Surprisingly, a firm that has been breached multiple times sees a decreasing effect of the privacy breach on its stock price. So that seems to reinforce the fact that firms learn and kind of use a little bit more the media's trove that they had available in order to attenuate this effect.

But where it’s very interesting is if you look at the effect of an additional piece of positive news story compared to the usual amount of positive news on any other day, you find an effect that is 15 times higher, like the effect of a positive news, an additional one, is 46 basis points on the day of disclosure of a privacy breach versus only three basis points on any other day. And this is very consistent throughout the entire sample.

So you notice, this completely offsets the negative effect of the privacy breach that was around, like, minus 24. Surprisingly enough, the market capitalization and the number of records breached, when available, do not have any effect on the result.

Something interesting, too, is that the result varied by industry. There's more of a negative effect for financial firms than there is for just like

the retail industry, for example. So this could be due to a strategic and sensitive component of the data that the firms have got stolen.

So the effect of stricter disclosure laws that are different in every state, as I mentioned, is significant and negative. So on average, it decreases the returns on the stock price by 17 basis points, so this can be in a way thought of as a partial insurance for the firms by knowing that if they have a privacy breach disclosure, they're going to have to release it to the market more quickly than in other states. So this may seem that firms would actually spend more time protecting themselves when there are stronger disclosure requirements.

So in a similar manner, you find that this effect is even stronger the day after the disclosure. We're talking 70 basis points. So if a sample were restricted to cyber attacks, because it seems to be, like, the topic of this panel, instead of all privacy breaches, all of our results that are mentioned -- and you see that in the paper -- are stronger, like twice as much of a negative effect on the release of a privacy breach.

These results could actually be due to the fact they are more sensitive information that are

coming out when you have a disclosure of a privacy breach that is obtained through a cyber attack. To give you an idea of how different privacy breaches and even cyber attacks are, I ran a similar type of analysis on different types of negative news to the stock market. And what happened is only a analyst downgrade would have a stronger effect on the stock market -- on the stock price, sorry, of the firm. So congressional hearings, copyright infringement, fraud, industrial events, lawsuits, even product recalls do not have as strong of an effect and most of the time are completely insignificant.

So this is really, like, quickly what's in the paper. You can find the paper online. And thank you for giving me the time to talk about it.

MR. HO: And thank you, Sebastien, for that insightful piece on the impact of data breaches on firms.

Next, we're going to move over to Al, who will be giving us his perspective on the impact of data breaches on consumers.

2018 Identity Fraud Study:
Fraud Enters a New Era of Complexity

MR. PASCUAL: Thank you. So, first, I wanted to thank the FTC for having me today. I'm

going to be sharing some research from Javelin's Annual Identity Fraud Study as background. And Javelin conducts a national study. We've conducted it annually for nearly 15 years where we examine the incidents of identity fraud affecting consumers.

As a definition, identity fraud is when personally identifiable information is misused to attain something of financial value. In essence, it is financial fraud that's made possible through identify theft. And for the sake of today's conversation, I'm going to be talking a lot about the relationship between fraud and data breaches.

That relationship is strong. It has historically been strong, but fraud itself is changing. The role that breaches are playing when it comes to fraud is changing, and I think it demands a change in the way that we deal with breaches and we also deal with the protection of consumers' data and consumers' accounts.

We've been following this space for a very long time, the fraud space. 2017 stood out. 2017 was, in fact, a record year. More consumers than ever before, at least as far back as we've been keeping records, were affected by identity fraud, right, in absolute terms and as a proportion of the population,

or at least U.S. consumers. That was a record.

The amount lost in 2017 was the highest we've seen in the last four years. Now, these are total losses associated with all cases of identity fraud. It is inclusive of losses that consumers are experiencing as well as the businesses where these frauds took place. But a third piece of information that I think speaks very highly of why we're seeing some of these trends play out is that for the first time, when we ask consumers who are affected by a data breach who received a notification what kind of information was lost, for the first time, we saw that Social Security numbers were at the top of the list. Historically, it's been credit cards and debit cards.

Now, we need to consider that there are 247 million U.S. consumers. There are 1.2 or so billion cards in circulation. And, historically, cards have been a high-profile target. It is typically pretty easy to access data. Generally, it's poorly protected, but the fact of the matter is consumers were more likely in 2017 to be told your Social Security number has been compromised than your card, right, and that's saying something when most people have about eight cards in their wallet.

Not only did it have a material effect on

the type of fraud we saw, but it's also having an effect on the consumer psyche. The type of information being compromised, the source of that information, and that is also very meaningful. We'll talk about that first, and then I'm going to move into some trends around the fraud and the relationship between breaches and fraud, how it's being perpetrated.

But I wanted to start with the consumer aspect. So when we're trying to measure the impact on the consumer historically, you know, one of the first questions has been -- well, I guess, show me the money, right? You know, what's the financial impact on the consumer?

Well, in 2017, the financial impact more than doubled from the previous year. On average, consumers paid out of pocket $104, those who were affected by fraud. Now, it may not seem like a lot, but when you consider we had -- well, more consumers than ever before, I think the total comes in somewhere between $1.5 and $2 billion that consumers paid out of pocket, so it’s not an insignificant amount of money that we're talking about.

And it's true that the median loss is actually zero because many people experience card

fraud, but you have to imagine given the size of that population and the fact that the median loss is zero, how many outlier cases have to exist that pushed the mean up that far in a single year? This is a function of the change of the types of fraud that we're seeing become quite popular, and so I'm going to dive into how different fraud types are changing, but there is a meaningful effect for many victims of fraud in actual dollars and cents, right, so there is harm there that we can measure financially.

When we talk about breaches, I think it's important to consider that everyone in this room has probably received a breach notification or seen a notification in the news that indicated they may have been affected by a breach. So 2017 was not unique in that consumers generally had experienced breaches before, right? This was not a new phenomenon for us to get a breach notification, so why was it different? Why has our common vernacular changed as consumers? Why are we more concerned about cybersecurity? Why is our mind-set changing?

Well, I think, first, you have to consider the type of information that was compromised in 2017. It was a bit different than historical, but on top of that, I think what ended up happening in 2017 was that

there was a change in the consumer mind-set because we did not have clear sight lines as consumers as to what the breach meant for us.

Well, in the past, big breaches were generally card breaches. Now, we did have, you know, large breaches of Social Security numbers here, you know, and there, so certainly there was OPM, there was Anthem, but Equifax was unique in the number of individuals that were affected and two other facts.

Number one, we have no control as consumers over whether or not Equifax has or had our personal information. Right, and that's true of all the credit bureaus and a number of other companies as well, but on top of that, that information that this company in particular held had to do with our financial wellness, so consumers were extremely concerned. They wanted to know what does this breach mean for me.

So if you go back through the Google search results and you look at the search index, what you'll see is when the breach occurred, the search index goes through the roof. People went online. They wanted to know what does this mean for me. There was a lack of understanding, a lack of awareness there despite the fact that we've been breached so many times. Think about the number of notifications, the number of times

your information has been breached in the last ten years. You're not new to breaches as a consumer, but consumers had more questions than they had answers last year.

And we can see that there's an impact, right, on how they view breaches and the steps that organizations are taking to keep them safe. So we ask a number of attidunal questions around data breaches. And one of the agreement statements that we have within the survey is that data breach notifications merely help organizations save face or meet their legal requirements and do little to protect me. The agreement with that statement grew considerably year over year between 2016 and 2017.

Now, consider, again, your own personal experience. When you're receiving a breach notification, many of them look alike, right? They include pretty basic information about details behind the breach and information potentially about the credit bureaus to contact, right, maybe even to contact the FTC in the event of fraud, right, but that's it. I mean, that's what we see time and time again.

Meanwhile, that last slide shows that people had a lot of questions, questions that were not being

answered despite getting those breach notifications over and over again. So it would seem that consumers do not feel as though the way that we respond to data breaches, the way that organizations respond to data breaches in notifying them is sufficient. They do not believe it is sufficient, or at least that sentiment is growing, and it has grown considerably. And I think part of the reason why it has grown is because consumers are more concerned about what a breach means for their identity.

We also ask about in the study concern around identity fraud, and concern around identity fraud also grew considerably. Now, typically, these are numbers that don't move very much year over year, so this is extremely meaningful. Going back to the earlier comment around the common vernacular, I think as consumers we have a much more keen realization that the information that's being compromised online, right, in the digital space does have more severe implications for our identity because we do so much online and so do criminals, do so much online.

So when we see that our information is breached and when we receive a notification, it doesn't tell us enough about what that means for the digital world where that information can and will be

misused, so we're starting to tie all these pieces together as individuals, and we're seeing that reflected in our data.

And the experiences around fraud kind of back up that notion. It's not as though we're taking a leap of faith as consumers. Fraud is just becoming more prevalent, and we know, right, if you have been a victim of a breach before, odds are your information has been misused to commit fraud, so you know that there's a connection there.

In this chart, what you'll see are two different sets of bars. The blue bar is the fraud rate for all consumers in any 12-month period, any calendar year. The beige bar is the fraud rate for consumers who were notified of a data breach. Now, there's a strong correlation. There's always a strong correlation every year. This is not causation necessarily.

And there are a number of factors that push that bar up and down, but the fact of the matter is there is the relationship, it is very, very strong. And if I included the data for consumers who did not receive a notification, you'd see that the rate is typically between 2 percent and 3 percent every year. So there is a very, very clear relationship.

Now, in 2017, you may ask why did the rate go down. Well, it's very simple. That number is a function of the number of breach victims who experienced fraud over the number of breach victims. The denominator became very big in 2017. There were a lot of breach victims who had sensitive information compromised. Criminals simply couldn't use it all, and that's why that number declined. The fact of the matter is there is a strong relationship and we know it, so we are more concerned.

So we talked about the consumers. I do want to shift into how this information is being misused, how it’s manifesting, and I wanted to focus on, in particular, a couple different types of fraud. The first is account takeover. Account takeover is among the most meaningful and insidious types of fraud for both individuals and for organizations.

So what do we mean by account takeover? Account takeover in this context is when a criminal gains effective control of an account. They will do that by changing contact information, by changing passwords. Essentially separating you as an individual from the organization that's servicing that account. And this makes it extremely difficult for that organization to ever provide that control of the

account back to you because they cannot discern the difference between the legitimate consumer and the criminal.

This kind of fraud has tripled. It's tripled. Losses have grown considerably, and incidents have grown considerably. Now, you may ask, what does this have to do with data breaches. Well, two things. First, criminals can leverage personally identifiable information to gain access to personal accounts. And, unfortunately, there are still organizations that allow you to gain access to an account with a Social Security number.

Tie that in with a bit of social engineering, someone calls up the call center of an organization with that Social Security number, and they can typically get a customer service representative to do a lot of things, including providing access to the online account, resetting passwords, effectively giving them a foot in the door to gain control of an account, but it’s not just the more sensitive personal information. It's also information like user names and passwords.

You wouldn't think generally, because we place so much value on Social Security numbers, that a user name and password is really valuable information,

but then think about how often you reuse a password. Well, criminals know that, and so they breach organizations. They take lists of user names and passwords, and in an automated fashion, they will basically use that list. They will take those user names and passwords and ping sites of different organizations -- banks, retailers, mobile network operators, healthcare providers, insurers -- until they find pairs that give them access to an account.

Breaches are contributing to this trend along with, in essence, very poor authentication controls. And I know Marc talked about it just a bit, but the fact of the matter is weak authentication is prolific, it's ubiquitous. We actually conduct another study on authentication, and what we define as strong authentication among businesses that have a digital property, adoption's in the single digits. Most organizations rely on a user name and password, and criminals use that to advantage after breaching information like user names and passwords.

And the other type of fraud I think that's worth mentioning in the context of breaches is new account fraud. For folks who work in financial services or related industries, you may view this as application fraud, but in essence it's where a

criminal takes personally identifying information and opens an account as though they were the victim. This type of fraud is also on the rise. This is a lot easier to connect, I think, in our minds with a data breach. We understand that personal information is compromised; they put it into a form online; they've opened an account.

But what I think is more interesting here and is much more problematic for the consumer is that the fraud itself is changing. The reason they're opening accounts, using information that's compromised in a breach, is changing. So you'll notice that the incident rate grows, but the amount lost does not. So we may view that as a good thing inherently. Less money has been lost, but there's a reason why.

More consumers are being affected by this type of fraud, but less money is being lost. And that's because criminals are opening accounts that in and of themselves have no monetary value. So what you'll see here are the number of existing account fraud victims, so consumers who have had an existing account -- it could be a debit card account, it could be credit cards, it could be a loan account, it could be an investment account, the number of existing account fraud victims who also had a new account

opened using their personal information.

Criminals value the complete identity of an individual. And we're at a point where the complete identity of pretty much any person in the United States can be found online. And what criminals use that information for is to get paid, right? So they have information that gives them access to an account where you may have your retirement, but they also have information they can use to open a new account.

Why would they do that? Well, banks check, organizations check, to see where money is being sent. And this is just an example. There are many reasons why they would, but consider if a criminal has access to your account, right, that has your retirement in it and they want to move tens of thousands of dollars, there are going to be pretty strong checks in place.

And what banks and other institutions will do is they will verify ownership of the destination account. And there are third-party services that provide that verification. Criminals know that, so armed with all of your personal information, they will open up a new account. It will have information that matches the compromised account. So when banks go to verify the destination account, it verifies and money is moved.

And it doesn't have to be something as grand or as sinister as draining a retirement account. It could be something as simple as opening a Paypal account to monetize a stolen credit card, to monetize a stolen checking account. We've seen this kind of fraud grow considerably, and criminals are opportunistic. They have all the information they need. Authentication controls generally are weak, and identity verification is also generally pretty weak.

So the long and short is that there is a very strong relationship between breaches and fraud, and that has not necessarily changed, but what has changed is the nature of the data that's being lost and how that information is being misused. And for consumers, we recognize that at least on a subconscious level, but many of us are also being affected. There are steps that organizations can take to change this paradigm.

Unfortunately, though, not all of them are regulated in the same way. There is nothing that unifies their approach in keeping consumers safe, whether that comes to data security or protecting existing accounts or identities. And as such, we have seen fraud respond and take advantage. And this trend will continue until organizations improve their

security postures, and we are all going to suffer until that comes. Thank you.

MR. LUPPINO: Thank you, Al. Thank you for all your insights on data breaches and resultant fraud that consumers experience.

I'll now ask does anyone have any followup comments, either on your own presentation or one of the presentations of the other panelists?

(No response.)

MR. LUPPINO: Okay.

MR. HO: So maybe we can start with a question. I couldn't help but compare Al's research with Sebastien's. And, so, you know, if Sebastien's research suggests that firms can or do essentially offset the negative consequences of a breach and, you know, that suggests perhaps they're not internalizing the cost of a breach and Al's research, to me, seems to suggest that consumers are experiencing harms associated with data breaches, so if, you know, these two situations or research are correct, then, you know, is there essentially a market failure? And I'd be interested to hear the panelists' thoughts.

MR. PASCUAL: Well, I think, you know, you have to consider Sebastien's comments when you start talking about market failure. It does not seem as

though there are the proper incentives in place for organizations to change the way they do business. And, you know, as a result, we continue to see breaches occur. And it's not as though criminals are incredibly inventive. They do the same thing over and over again, moving from organization to organization. And, I mean, that's what keeps the folks at Verizon, I'm sure, very busy.

MR. SPITLER: Yeah, certainly with the financially motivated ones. You know, you have the ability to be opportunistic because it’s not necessarily “I need this set of Social Security numbers” or “I need this set of payment cards,” whereas the ones that are looking more for trade secrets, then it’s going to be a lot more targeted. But, yeah, as you just said, so they don't necessarily need to evolve so much. It's more like, oh, well, that guy raised the bar up to here. I still have a lot of low-hanging fruit that I'm able to reap, and I can pull that and still make money.

MR. PASCUAL: As far as the organizations that are being affected, surely governments are affected. Nonprofit organizations are affected. But for businesses, I mean, what we’ve historically seen in our data is when they think about security, you

know, the top motivating factors for them are whether or not it's cheap and easy, right? When they're making decisions about what they're using, cheap and easy tend to, you know, go right to the top of the list, and that seems to be incompatible with protecting, you know, the needs of protecting the data that they have, whether it's their own or consumers.

MR. GAY: So at the time when I was doing my research, something was emerging, like the relationship with insurance on data breaches. And you could see a pattern where there was actually a mismatch between people's insurance, like pure insurance against data breaches, and also the amount of media that they were using in order to, like, alleviate any effect of data breaches.

So, now, I don't know if both of you guys are aware about the more, like, formed market for cyber insurance, for example. Because before there was a real mismatch. When doing that research, people didn't know what they were insuring themselves against, and then insurance companies actually didn't know how to price it properly.

MR. PASCUAL: And I think that's going to be one of the forces that actually improves security postures because insurance companies are and will be

more likely to demand better security among the companies they are insuring. Obviously, there's no absolute security, but if you're going to indemnify an organization, you want to be sure, at least to some extent, that the risk is as low as you can manage.

MR. LUPPINO: Do you see in the data the same firms experiencing the same types of breaches over time? And based on your research, what evidence do you see of learning in the market by firms and consumers?

MR. SPITLER: Yeah, so I don't know if you're referring to the exact same organization --

MR. LUPPINO: Yes.

MR. SPITLER: -- the exact same breach? I'm sure that happens. The interesting thing with my data set is the majority of it I actually don't know who the victim is. So, for example, when the Secret Service provides me information on breaches that they've responded to, I get demographic information and I get, you know, obviously the tactics used, et cetera, but I don't get who the end victim was. And we don't need that for us to do our work with it, and that allows us to keep the anonymity of it.

I'm hopeful, you know, that in a lot of these cases some of these breaches -- again, they go

to things that aren't necessarily earth-shattering. There are breaches that occur that it's a fairly straightforward and simple fix that could have at least broken that particular event chain. There's nothing to say that they can't circle back and try a new avenue, so I don’t know.

I'm hopeful because a lot of times we're not seeing what I would call highly sophisticated attacks. A lot of these are very opportunistic. It's going after weaker configurations, weak authentication schemes, so there's a higher chance that they can learn from their mistakes. And I'm hoping that what my report does is allow people to learn from the other guy's mistakes, so, again, but I don't have any sort of hard data percentages on that.

MR. HO: I want to switch gears a little bit and ask Al a question about one of his slides. It seemed quite interesting to me that you pointed out that there's a cynicism with consumers about data breach notification. And so, that, to me, seems a bit counterintuitive, but maybe you can sort of elaborate as to sort of what you attribute to this cynicism and, you know, how if -- I guess how would you improve data breach notifications if this really is the case with consumers.

MR. PASCUAL: So I think part of the challenge is that we've all gotten, to my earlier point, notifications before. The notifications we continue to get look very much like the old notifications. And in and of themselves, there's just -- there's no longer any remedial value for the consumer in those. They're not going to learn anything new by reading the newest breach notification. All they're going to learn is that they were breached, in essence. I don't think they even care what happened, right? In fact, there may be so much spin, you know, after the breach is announced, that they have a hard time making out what actually happened in the first place.

The challenge ultimately is that for consumers, we are more aware of fraud, we're not being provided with anything in the event of a breach that makes us feel as though we're going to be safer. And, so, you're getting a piece of paper, and how many pieces of mail do we all still get, right? It feels very kind of perfunctory, something that has to be sent to us but doesn't give us anything.

I don't know if changing a piece of paper is going to make consumers feel much better. I think it's more about providing something to them that makes

them feel as though they will be safer. At the same time, you know, if breaches continue to occur in much the same way from organization to organization, the kind of information continues to be lost everywhere and consumers don't feel like they have a lot of control. Giving them all the identity protection in the world still isn't going to totally undo their cynicism, right, because a problem still exists. And what am I going to do after I have five different identity protection plans? I'm probably going to be pretty cynical about that, too.

MR. HO: Anyone else have any comments on that?

MR. SPITLER: I would probably look at it kind of as from a consumer, not necessarily from the researcher, but, yeah, kind of what you said, it's almost like, oh, yet another form that I'm getting, and I can see that you've given me a year credit check. Okay, but there's nothing in here that shows me or gives me any sort of confidence that you can understand why it happened in the first place, that you have controls that are -- what's going to be different from you and from the people that work in your -- your security practitioners that are going to prevent me from getting another one of these pieces of

paper one year, two year, three years from now? So you don't really get that kind of warm and fuzzy feeling from them.

It's just more along the lines of, oh, they have to do this, so here's my obligatory piece of paper from them, but I'm not getting any good sense of, yep, we know what happened, we've made steps, and, you know, this type of thing. You don't get really a good -- it's not really confident that it's just not going to happen again.

MR. PASCUAL: A piece of paper does not tell you what the risk is to you. And we cannot possibly expect that every piece of paper we send out to an individual is going to be customized to their risks. And it feels almost like something that needs to be solved, and digital is part of the problem, but I think it's also part of the solution.

You know, having an understanding of who the consumer is, where they do business, what that breach could translate into ultimately as far as fraud is concerned and providing them with real solutions for their digital life, that is not a piece of paper. That's something totally different. Right now, people pay for that kind of thing. And, again, not to say identity protection is a solution we need to be

throwing on people, but I don't think you can improve the notification enough to undo the cynicism.

MR. GAY: And back to the research that I've done over that sample, 2005 to 2014 data, the issue is also that the states have different requirements, so you end up with the key question, like which one takes precedent. If you have a multistate disclosure issue, then questions get raised. I don't even know the answer to that, and I think it’s usually very contentious.

In terms of breach fatigue, that's also something that you could find in the sample. Early on, when there were not a lot of privacy breaches, the effect of those breaches were higher, like I gave you the average number, that was 24 basis points, but it could go as high as, like, 60 or 70 basis points in the early years. Whereas the closer you get to 2010 in the sample, then the smaller that particular effect. So this is also an interesting trait, I think, there are more and more breaches.

MR. LUPPINO: So piggybacking on this, you know, if consumers are becoming more cynical about things like breach notifications from companies, do you see changes in their behavior, or are they becoming more -- do you see anything as far as they’re

becoming more proactive about their data security or other kind of changes to their market behavior?

MR. PASCUAL: We track behaviors pre- and post-fraud, for example. We noticed a rather disconcerting trend that two or three years ago, historically, when people experienced fraud, one of the first things they did was, you know, they shut off all their paper statements and they went online because they just didn't want things going through the mail. Starting a few years ago, it kind of went the other way, where people, after they experienced fraud, would stop banking online, like, they'd stop using online services. They had a fear that that's where the risk is.

And that's problematic because digital allows individuals to do so much. I mean, obviously, it obviously allows businesses to reach a wider population. But, you know, that being said, we tend to be very reactive as consumers, so post-fraud we see people do things like get identity protection. We see them, you know, step up their security posture. They take advantage of two-factor authentication.

If you use Gmail, I mean, Google has come out and said less than 10 percent of all Gmail users use two-factor authentication. I mean, if consumers

were really demonstrating some of the concern that we see in the data in their security behaviors, I think the adoption of two-factor authentication with Gmail and other online services just generally would be higher. It's not.

People are concerned. I think there's just a disconnect between knowing what they should be doing, right, and what they're actually doing. So we see them do things only after they experience fraud, but beforehand, it’s kind of -- there's no rhyme or reason for them.

And I think that speaks to the fact that they need more education. They need more understanding of what the implications are for them and what they can actually do. But as our digital life continues to expand, that can almost seem, like, overwhelming. We have a unlimited number of digital accounts. If you have to protect your entire life, that's a tall order.

MR. HO: Okay. So, actually piggybacking on that, so if individuals only respond after experiencing a breach, right, you can also think about in terms of firm responses. So going to Sebastien's research about market, is it possible that the market is just confident that firms will take appropriate

measures to eliminate the vulnerabilities discovered by a breach?

MR. GAY: So you know I cannot answer that, right? So based on my research, what you find, though, is there's a high likelihood that firms have a store of, like, positive news that they hold on. So I don't say it's something they have to release, but it could be something as announcing a joint venture. It could be something as simple as the nomination of someone buying a particular type of widget that it could wait a month or so. And you see that in the data, too.

So if you look and do a word analysis, you notice that those are the types of news that come out or expectations about future earnings most of the time. So this is something that is done. Whether or not it is done on purpose, obviously there's no answer to that, but it is just surprising that on average this is the sort of result that you would find.

MR. HO: Did anyone have followup?

And, Sebastien, this is actually a question from the audience. It‘s a followup to your research. What breaches are not represented in the news that you have found that you discuss in your paper? And, you know, is there a trend by size or by industry?

MR. GAY: So I'm going to answer the second part. It was already difficult with the sample to have size. I mean, less than, like, 50 percent of the sample had actual numbers, even estimated numbers. So most of those breaches, I think currently it is more often than not that we get an idea of how many people have been breached. So for some breaches that were not reported in the news, it was mainly a loss of like a laptop, for example. Someone forgot, like, a laptop on a train.

And that was reported on people's websites but it didn't make it as a news event, and I cannot recall the company, but that was that type of issue, which the laptop contained personal information for the people that were working at that company. It was a member of HR, but perhaps because no one knows whether or not it was breached, there was no report in the news.

MR. SPITLER: I can touch on that a little bit just from kind of the data that we get in. When you look at -- you know, we have a category of lost and stolen assets. And the two industries that are very prominent in that are healthcare and public sector. And we go out of our way in the report to say, hey, we are not saying that I think healthcare

workers and people that work in state, federal, and local governments lose their laptops more than anybody else, but they have to disclose it when they do.

And, so, we have a lot of data on industries that have to disclose things like that. So that's why you'll see such a high level of -- you know, it is so easy for us to find healthcare breaches, just even using open-source methods. We don't have to worry about some of our other partners providing it to us. We do similar things when we look out there and we look for publicly disclosed data breaches. And that is part of one of the data sets that goes into the full report. So there's a lot of that is tied to what industry and what type of data.

MR. LUPPINO: Here's a question from the audience. For the Javelin estimates of consumer costs from breaches, who pays the costs? Is it only consumer costs, or are some or all the costs borne by firms?

MR. PASCUAL: So the larger number I shared, I believe it was 16.8 billion, that is inclusive of all losses. Now, consumer costs are a portion of that, and there are some costs that are not necessarily reflected in the larger numbers. So consider that 16.8 billion is really direct losses.

For consumers, you have both direct losses, cases where they reported fraud and an organization said no, you pay it, because that can happen despite federal regulations. You know, there can be cases of fraud, especially new account fraud, where the consumer cannot, in essence, prove that they were not responsible. Right, that burden of proof practically falls on the victim. But on top of that, I think that's a good example to use.

In the case of new account fraud, I may need to file a police report, so I take time off work. I may need to get a lawyer. And, so, I have additional costs beyond what the fraudster actually got away with, and those, you know, can be borne and typically are borne by the consumer. And that's still, you know, a billion-dollar-plus problem.

MR. HO: So we've been talking a lot about the cost of data breaches. And I want to move over to the attack vectors for data breaches for a moment. And this is in part a question from the audience, but I'll sort of add a little bit to it as well. So, you know, first, we've seen this increase -- you know, from Verizon's report, we've seen this increase in social engineering. And, so, I'd be interested in hearing how phishing and social engineering attacks

have become -- whether or not they've become more sophisticated over time and, if so, sort of how.

And then tacking onto that the audience question, has Verizon observed any measurable differences in the frequency of attacks or use of particular attack vectors when accounting for particular operating systems or server types?

MR. SPITLER: Okay. So the first question kind of regarding phishing and social engineering, and when we have social engineering involved, probably 90-some percent of the time it’s actually phishing. And the reason for that is it works. So we have data from multiple security awareness training vendors. So you hire them. They'll actually phish your users, and just tell you who took the bait, who didn't, how good are you doing, are you doing better than the last time we did this, et cetera, et cetera.

And it was about a 7 percent hit rate for any -- so we sent a campaign out. Of all those emails that were sent out, 7 percent of them someone will take the bait, so it works. And it's also very easy to do. It's a very low-cost, very efficient style of attack. And, you know, if it doesn't work, oh, well. You'll just try to phish the next person, right?

And, so, that's why we continue to see that

coming up. It's a very good way of -- and we also take a look at how networks, you know, are kind of set up, right? You know, we have some web servers over here, and they get direct interaction from anybody on the internet. Well, how could I interact with someone's workstation? Well, I can do that via email, you know, and so it's a great way to try to get a foothold into a corporate network.

Now, as far as level of sophistication, it kind of runs -- it runs the gamut. You're always going to see the just throw it out there, the actual just phishing. Let's see who will actually take this bait. You know, you will see targeted phishing attacks. It's called spear-phishing is kind of the terminology for it. And that’s when you’re not just sending it out to anybody, but you’re sending it out to a specific person because of the rule that they have. You've probably done some gathering of intel via their LinkedIn -- you know, their LinkedIn pages or other social media.

So it allows you to kind of craft a narrative to make it a higher likelihood that they're going to click that. Hey, oh, I think you're going to go to that blank conference. Here's a PDF, you know, of the agenda or some afterparties or something like

that. It's topical. It's not out of the blue. And it's something that, you know, you'll go ahead and click on.

And then the second part was in regards to --

MR. HO: Just sort of the measurable difference, if you've seen measurable differences in the frequency of the attacks.

MR. SPITLER: Oh, based on operating system and things like that? Often, we don't get that level of detail. Now, there are certain -- you know, there's certain -- you know, I'm not going to get into any sort of this operating system is better than or worse than that operating system. Frequently what we see is not necessarily weaknesses in the way that the underlying system code was developed, but we see weaknesses in how people have implemented that in their environment. So, you know, a lot of times, it is a weak configuration, not necessarily a software-coded bug, which would be, you know, specific on one OS versus the other.

You know, there are certain types of vulnerabilities that might be exploited more often than others, and we've seen things like that. You know, browser-based vulnerabilities are ones that, you

know, if you are -- those are ones that attackers like to go after because they've had good success with that in the past. And, again, it gets you onto a particular device in the network.

So we will see some, you know, some weaknesses exploited with more regularity than others, but it is not a, you know, this OS versus that OS or this type of web server versus that type of web server, at least not to where I can provide any sort of guidance or hard numbers on that.

MR. LUPPINO: This is another question from the audience. To what extent is there evidence that those who steal data in large sophisticated breaches with Social Security numbers and full identity data, how do they monetize that day-to-day? Do they do it gradually, or, I mean, do they try to monetize it immediately? Do we have a sense of that?

MR. PASCUAL: Generally, they fall into a couple camps, right? You have cases where data is compromised and that individual organization looks simply to sell the data, right? They have no desire to commit fraud in any way, shape, or form. They're going to realize values by selling it on, you know, the open market. So whether that's forms on the deep web or on the dark web or wherever.

They may do some testing of that information. So they'll take -- let's say they get a list of user names and passwords. They'll test them at big banks, right, and, you know, they'll see how much money is in those accounts. In the accounts where there's weak authentication and plenty of money, they will price those credentials higher than they will other credentials.

Same thing with credit cards, right, higher limit versus lower limit cards. Higher limit cards are worth more. Lower limit cards are worth less. They'll even do things like package them up by zip code because they know that banks and credit card issuers will do verifications of, you know, where the cards are used relative to the zip codes of the owners. And, so, they'll do additional steps to make the data more valuable, right, to different criminals.

So you have that population, and then you have those who compromise the information to misuse it to and actually commit fraud. Those tend to be more vertically integrated organizations, so they have the capability to both glean information and then to put it into use, whether that's opening new accounts online or even -- it’s less popular today because of EMV chip cards, but, you know, take card data, put it

on what they call white plastic, which is just kind of like blank cards or gift cards, and go to the streets and start using it.

But you tend to see more breaches are committed -- the theft of personal information is more likely to be committed by organizations that are not planning to commit fraud. It's generally very different skill sets, but you do have vertically integrated organizations who will do all of it.

MR. LUPPINO: Thank you.

MR. HO: Okay. So I'd like to conclude with one final question. And I'll try to combine some of the audience questions with it. So we've been doing a bit of discussing about the current trends related to data breaches, but I think we'd love to hear what your guys' thoughts are about the future of data breaches, what they look like, or what you see them looking like, you know, like five years down the line.

And, then, you know, on top of that, what would be your number one advice to firms and businesses for how to avoid breaches or protect themselves?

MR. PASCUAL: So I think from my perspective, breaches will continue. I think it's not just going to be the personally identifiable

information. It's going to be anything that's not nailed down, including biometric data, right, as that becomes, you know, more often used for things like identification and authentication. We'll see, I think, a bit of a shift in tactics depending on how well that data is being protected. So you'll see organizations over time increasingly protect data with encryption and tokenization.

And I don't think that wholly dissuades criminals, right, so making that data, you know, harder to misuse -- now they may target organizations that have yet to protect data in that way more often, right, rather than going after the harder target, but there's always the opportunity to do things like take advantage of user privileges and get access to data within the network, right, that’s supposedly encrypted. So, you know, there are going to be steps that are going to be put in place to protect our information. It's not a panacea. But because information always has value, personal information, as well as IP, you know, business bank account information, it's all of value, so breaches are not going to go anywhere. This is going to continue to be a problem.

I mean, I think you'll even see in other

places like Europe where more strict data privacy regulations have been put in place that breaches don't go away in totality. I think you'll probably see fewer consumer-level breaches, but, you know, more targeted attacks to get, you know, information that an organization really wants to have, whether it's espionage, corporate espionage, I don't think, you know, something like GDPR is going to necessarily be the most effective tool for moving the gauge and getting businesses to better protect that information.

MR. HO: Anyone else?

MR. SPITLER: Okay, so, crystal ball, I am hopeful that some of the things that we are putting into place to make it harder to monetize stolen payment card data, so, you know, we're still going to have these breaches, but in reality the whole story doesn't stop there. Granted, your work, it's what happens after the breach. How are they going to make money? How can we just -- this is kind of our economics and how do we defend against them?

And then from this point, this is their economics and how do we ruin this or how do we make it a lot harder, like most notably with card-present fraud. So he talked about, you know, being able to clone cards, white plastic, things like that. If we

can reduce the effectiveness of that, that's going to have to cause them to change their plans a little bit. I could see that then putting a higher value on personal information to do tax type fraud, the account takeover, new-account-type fraud, if they're not making the same return on their investment that they were with stolen payment cards.

And, also, some of the monetizable events that don't necessarily require a data breach. So are they going to -- you know, a lot of times, things aren't new, it's just kind of nuanced. So are we going to have other different styles of kind of ransomware type of attacks where they're going and they're holding the utility and the availability of something to be able to make a buck? So I'm thinking that might be the way that they would go.

MR. GAY: Just I can only highlight obviously what was in the paper, but the idea is a good look at the disclosure laws by state would be a thing to think about and also looking at the mechanism that firms have in order to, like, attenuate the impact of privacy breaches would also be something that at a time I was advocating.

MR. HO: Well, with that, I'd like to thank our presenters for their thoughtful comments on these

very real and impactful issues.

With that, we're going to be breaking for lunch. There's a cafeteria located on this floor. Please remember that if you leave the building for any reason, you'll have to go back through security, so please plan accordingly. And we will recommence after lunch at 1:00 p.m. Thank you.

(Applause.)

(Recess for lunch.)

INCENTIVES TO INVEST IN DATA SECURITY

MS. JILLSON: Welcome back from lunch. Our first panel discussion this afternoon will address incentives to invest in data security. And we are fortunate to have with us today five panelists who have thought a lot about this topic. First, my name is Elisa Jillson. I'm an attorney in the FTC's Division of Privacy and Identity Protection.

Next to me is my comoderator, Mike LeGower, who is an economist with the FTC's Bureau of Economics. Our first panelist is Lawrence A. Gordon, who is the EY Alumni Professor of Managerial Accounting and Information Assurance at the Robert H. Smith School of Business, University of Maryland, College Park. Dr. Gordon is the author of the Gordon-Loeb model, which provides an economic framework for deriving an organization's level of cybersecurity investment, and he will be describing that model today.

Next to him is Matthew P. McCabe, the Senior Vice President and Assistant General Counsel on Cyber Policy for the insurance broking and risk management firm, Marsh.

Beside him is Tyler Moore, the Tandy Associate Professor of Cyber Security at the

University of Tulsa. And next to him is Sasha Romanosky, who is a Policy Researcher for Rand Corporation.

And, finally, we have Matthew Sharp, the Chief Information Security Officer at Logicworks. Thank you all for being here.

And for the audience, if you have questions during the discussion, please feel free to write them down on your question cards and flag Ryan or Mohamad and they will collect your cards and bring them to the front.

Now, this morning we heard some presentations on the impact of data breaches, and presenters discussed whether there's a market failure in security resulting from misaligned incentives, where companies guard data but it’s consumers who bear some or many of the costs of breaches of their personal information. To think through this problem of incentives, we'd like to take a look at current incentives to invest in security.

So in this slide, there is a list of incentives. And, so, what I'd like to do, panelists, is to go down the panel and ask each of you if you had to name the number one incentive to invest in security, the most important incentive on this list or

not shown on this list, what would it be and why do you think that's the case? And why don't we start at the very end of the panel with Matt.

MR. MCCABE: Sure. Thanks, Elisa and thanks to FTC for having us up. Well, I'm in the private sector. And I have served in a capacity in a number of different organizations and also previously in two of the premier cybersecurity consulting firms in the country. The conversation or my opinions are probably biased by the opportunity to sit in closed-room -- closed-door sessions with CISOs where oftentimes I'm looking to learn from the guys who, you know, have the most, I'll say, street cred, if you will, the guys that are leading the largest programs in the country.

And pretty predominantly, what I've been coached to do and what I've made a career of doing is starting with value creation, so competitive advantage or customer demand seems to be the two that would be my preferred option. However, not all security investments are, you know, easily framed in those contexts.

MS. JILLSON: And when you say competitive advantage, you know, oftentimes we think of security in terms of a cost center. So how do you reconcile kind of that received wisdom with the notion of

security as actually an advantage in the marketplace?

MR. MCCABE: Sure. There's a number of firms and it really depends on your business model, but for example, at my current employer and these are my opinions, not necessarily representing the opinions of my employer, we have the opportunity to build a value-creating or revenue-generating service offering. So, for example, we have built a data loss prevention service that actually expands revenues.

But there are other companies in -- many of them are our customers, where they're inspiring purchases in their organizations by differentiating on their ability to protect customer information, so, you know, organizations out there that provide or support fintech offerings or healthtech or regtech. Many of the technology-driven organizations that are looking to disrupt industries often have the ability to differentiate, and the way -- one of the ways that they do that is by making sure that they can inspire confidence in their customers, be they consumers or B2B purchases, that they're going to value and treat the confidentiality of information as, you know, an important part of their business model.

MS. JILLSON: That particularly makes sense where an obvious feature of the product is security,

so if it's a cloud provider or let's say it's a manufacturer of a home security system. So security is kind of at the fore of what consumers or customers are looking for. Do you think that that holds true where security is not such an obvious feature of a product when a customer is buying shoes or a business customer is buying office furniture?

MR. MCCABE: Yeah, I think that there's some validity to the emotional responses in management that happen in organizations that do sell things to consumers. For example, you mentioned shoes. In my background, I worked for a shoe manufacturer, so I have a little bit of insight there. And, you know, no executive team wants to be distracted by a major data breach, and no executive team wants to lose the opportunity to grow revenues because consumers don't believe that their information is protected.

I think one of the panels earlier seems to indicate, at least from a market cap perspective, that that's not happening and that consumers, in fact, don't behave consistent with their best interests. However, that doesn't necessarily mean the dissent in management teams accurately reflects that reality.

MS. JILLSON: Sasha?

MR. ROMANOSKY: Hello.

MS. JILLSON: Going back to this slide. If you had to name the number one incentive on or off the slide, what would it be?

MR. ROMANOSKY: I think it's a great slide, first of all. And I think the incentives that you've listed here are pretty super. And I think the exercise of ranking them is interesting, and I think as researchers what we would love most is to be able to understand the marginal effectiveness of each one of these.

You know, I look at them, and for each one, I think we could have -- you know, we could spend the whole day discussing it. If we look at consumer trust and reputation, it's not really clear to me that there really is an effect of reputation. I'm not even really sure what reputation is, for example.

I think what people mostly mean is just sales. And, so, if we think that, you know, there's a loss of reputation, I think what most people interpret that as just sales.

We heard from the panel this morning that there was a loss in stock market price because of data breaches. I think there's also a larger body of work that suggests that, in fact, there is no effect from data breaches, and if there is, it's a very short-term

effect and then disappears after time.

The story of ex ante compliance and ex post liability, I think, is fantastic. I think there is -- there's a whole world of -- a body of literature on law and economics that talks about the benefits and limitations of each one of these and how can they be best applied, especially in situations like data breaches and privacy violations.

So, for example, ex ante compliance is useful when the inputs are strongly correlated with the outputs. So if we really believe that certain kinds of security controls will reduce the harms or reduce data breaches, then compliance is something that we should try and promote more and more.

Also useful when the injurers are known -- or, sorry, when the injurers are unknown. If we don't really have a good handle on who is causing identity theft, where the breaches came from, yet there's some amount of consumer harm kind of underlaying the community, ex ante compliance is good. Ex post liability, very clear when the harms are very quantifiable and there's property damage. When there's personal injury, and when the injurer is known, then you can bring actions against the company and recover whatever losses.

The ex ante compliance, better when the state has more information about the kinds of harm relative to the firms. The firms don't -- themselves don't really collect information about which consumers or employees are harmed in different kinds of way, but the state, so for example, FTC or a regulator, has broader information about overall population that suffers some kinds of harm. Ex ante compliance can be very useful.

If the harms occur long after the accident has occurred, for example, if that continuity, if that correlation is very weak somehow, compliance can be very good. I'll say that, however, so all of that paints a picture of how compliance could be very useful in the case of data breaches and privacy violations.

On the other hand, you know, it still seems to be a case that we're not very good, we haven't gotten good at understanding what these harms really are. You know, we heard earlier today, losses in the hundreds of dollars for consumers, average losses. It still seems to be true that most people don't lose very much at all, if anything.

And it's really kind of a failure on our part, on the information security industry, that we

are not very good at understanding what kinds of security controls really are effective. I think everyone in this room and certainly experts, we could all produce a list of technologies, of procedures that would help in some kind of way -- two-factor authentication, firewalls, intrusion detection, whatever, but nobody is really able to tell us which ones are more effective and by how much. We just aren't there yet. We just don't have the maturity as an industry.

Customer demand or customer demand for privacy and security, so this is a story of whether or not firms compete on privacy. And I think in one of the previous panels from a few weeks ago, there was discussion of whether or not firms actually compete on privacy, on security. And there was the argument that, oh, well, yes, they do, of course, because look at all the money that firms have invested in different kinds of features.

I'm not really sure that's evidence that there is a demand for privacy. At best, what we can do is highlight search engines like DuckDuckGo and talk about different kinds of privacy-enhancing technologies that exist in the marketplace. And it's nice and they're there and they work, but they haven't

really reached that kind of market penetration, right? They're certainly not competing with Google. They're certainly not competing with Bing. And, so, I'm not convinced that there is actually customer demand for privacy. I think if there was, we wouldn't be trying so hard to find it.

Insurance is a great field. And I think a number of us could talk all day on the benefits of insurance. I think that does provide, or at least in theory should provide, incentive for firms. They can enjoy lower premiums, they can enjoy broader coverage, they can enjoy fewer exclusions in their policies if they've adopted certain kinds of security controls. Again, I'll point out, we don't really know what those security controls should be, but, in theory, it should work and it should provide incentives.

And that could be a win-win-win for everyone. Firms are lower risk; insurance companies are more profitable; and overall social welfare is increased from fewer breaches.

So back to your question. You asked me, you know, which one of these is -- you know, could be the most powerful. I don't really have an answer. I haven't studied that. What I can say is that each one of these offers the potential for creating incentives,

but none of these alone, certainly from my mind, really sticks out as a major force driving firms.

MR. LEGOWER: Sasha, so you said something that I thought was interesting about reputation, and essentially that in your perspective it just collapses all down to sales essentially, right, that this is, you know, the business' reputation in the minds of consumers. But you can also think of an individual executive's reputation, right? So some individual executive as domain over the cybersecurity posture of a firm. And there's been some high-profile incidents recently where executives lost their job or had their communications exposed as a result of the data breach.

So can you talk a little about the extent to which concern for personal reputation might drive security? So we have all this research that says maybe business reputation doesn't matter so much, but, you know, if an individual executive's job is on the line, could that make a difference?

MR. ROMANOSKY: Yeah, absolutely. It could. I think that's a knowable thing. I would think what you could do is just ask a bunch of CISOs really what drives their incentives, right? That would be one way, and I think we'll get at some of this, and Tyler's done some great work on that, too.

It is also true that there aren't that many situations where executives have lost their jobs because of this. Certainly, in the Sony case, and the Equifax, and the Target, there have been, right, some embarrassment and some layoffs because of that. Although, I think in some of those cases, they did enjoy a bit of a golden parachute from leaving afterwards, so it is possible that the threat of personal reputation could drive better behavior.

I'm not sure I would be the best one to answer whether or not -- how much that affects the decision-making. I think Tyler would be better at answering that.

MS. JILLSON: And Tyler?

MR. MOORE: Okay, so hi. So I think Sasha's right and that each of these incentives you list I think have an impact. If I were to pick one, I would point immediately to compliance as being the single biggest driver certainly of investment in security. And when we talk to CISOs, they almost grit their teeth when they say it, but it's -- you know, they know that a compliance-driven mind-set to security doesn't lead to the best security plan and posture, but they also know that an argument for compliance is the most effective in getting the budget that's

required. It sets the floor for what you have to do.

And so much of what we do in cybersecurity and cybersecurity plans result from compliance demands, whether it's, you know, Sarbanes-Oxley, which shouldn't even necessarily have anything to do with cybersecurity but it has driven an entire emphasis on security among publicly traded firms or to more sector-specific compliance rules.

So that, to me, seems to be the strongest incentive to invest in cybersecurity writ large for companies. It's, you know, a fairly imprecise instrument, and it tends to set a floor and not a ceiling, in terms of what should be achieved, so there are definite downsides, but it does seem to be effective.

A comment about all of these incentives is that I do think they all have an impact. I think the real question is whether or not these incentives on their own are sufficient, and I would argue that they are not, taken as a whole, because of the presence of market failures, and, in particular, two market failures: the presence of negative externalities of cybersecurity and breaches.

So long as the harms resulting from a breach go beyond the affected organization who makes the

security investment decision, they will tend to invest less in security than would be socially optimal. You know, so take the example of Equifax. The data breach happened. It was bad for the company. Their C-Suite got replaced. And yet the harms to consumers, to broader society, to financial institutions is much, much greater than what Equifax itself, on its own, experienced when we view it collectively.

There's also information asymmetries in that we -- you know, it makes -- we don't actually have a good sense often of what an effective investment is, sort of following on Sasha's point about, you know, we have recommendations on different investments to make, but we don't know how effective one particular control is or not.

We also don't know often what the true magnitudes of certain kinds of risks are. In a certain sense, data breaches is kind of a positive exception to that because we have had, you know, more than a decade's worth of data breach requirements in force. We now know arguably more about the prevalence of data breaches than just about any other cybersecurity threat. And, so, that has certainly, I think, influenced boards and the sort of governance of companies to focus on preventing data breaches because

it has become so visible as a result of data breaches. So we see a lot more attention being paid to data breaches than we might see being paid to other forms of cybersecurity risk. So just the obligation to disclose, I think, serves as an incentive to make some investment.

MS. JILLSON: Matt?

MR. MCCABE: So I would opt for the top incentive to be reputation, but I would redefine it in a way that it's really reputation to your stakeholders. I think that's how certainly for public companies they think of it to their board and ultimately to their shareholders.

I mean, if you think about it, you have an organization that is a viable concern, hopefully a highly successful organization, and you have certain risks that you deal with every day. Some of it is financial risk, and you have the opportunity to plan for that appropriately. Some of it might be an ethics risk, and you have the opportunity to put in a compliance regime and to have governance over that to monitor it, but cyber risk for many of these companies, is kind of that unknown risk that can just take your legs out from under you.

And I would say that all these other

components actually feed into the company's -- in the C-Suite's ability to maintain reputation. What is our relationship with our customers? Are we meeting our compliance regimes? Am I limiting my exposure to large liability? Am I reducing cost? These are the items that all senior officers go through every day in order to maximize performance. So I think from a corporate standpoint at least reputation is the ultimate concern.

MS. JILLSON: And Larry?

MR. GORDON: Okay, so I would say I want to rename cost reduction to cost savings. I would say cost reduction over cost savings because you've got to think in terms of cost being implicit and explicit costs. So there are explicit costs of detecting and correcting; there are implicit costs. The implicit costs pick up ex ante compliance, reputation effect, and ex post liability. Those are a cost to a company, okay, if they have a big breach or a potential cost.

So, really, you can wrap up three or four of those right into the cost savings notion, so companies look at it from that point of view, but I think it was Tyler who mentioned one of the real issues is that a lot of the big costs are what we call implicit costs, the costs of, you know, with reputation, the way we

look at some stock market returns.

Unfortunately, these costs tend to be transitory. And by that I mean they're not permanent. Temporary stock prices drop down. Look at the big breaches we had. You know, take a look at Target's, for example. You know, their stock dropped down for a few weeks, and then it comes back.

But on the other hand, part of those costs is that there are executives who lose their jobs. The CEO lost his job. The CISO, you know, chief information security officer, she decided one month after the breach that it was time to retire, that she was planning on it any way. And we see that quite often. Actually, a lot of the security officers are the ones who bear the brunt, so what we have is an agency problem.

At least from my interaction with security officers, many of them, you know, they look at this and say, look, we need more security because I'm the one who pays the price. And from the chief financial officer's point of view, he or she looks at it from cost-benefit basis. So, you know, what are the benefits? What's the cost? And if the benefits aren't greater than the costs, we take a hit. It's an operating cost.

So I would say cost reduction because to me cost reduction includes compliance. If you don't comply, you've got a significant cost. Reputation effect. If you have a big breach, that's a cost to your company. Ex post liability is clearly a serious cost, and so you can wrap up many of these into cost reduction.

On the other hand, I would also say that all of these things are important. You know, so it's not like one doesn't count, but, to me, when companies look at -- corporations that I deal with, when they look at security, they're thinking in terms of potential costs. And they're thinking in terms of there's a cost to a reputation if they have a big breach. There's a cost to -- if you have a big lawsuit and you lose, there's a cost to not complying. There's a cost to detecting and correcting breaches, so all these things I put into cost.

MR. MCCABE: Can I just comment on that description? And, you know, this is perhaps a little oversensitivity, but to kind of back up some of -- our portfolio of clients and even our own company, I think it’s very rare that you have a CFO or a treasurer who says, look, you know, you just analyze the cost, and if we have to take a hit, we take a hit.

I just don't think that that's how companies think about this problem. I think what they do -- and to go off of Sasha's comment -- the hard part of this is the calculus of what's the overall efficacy of these protective measures. So there was a great post on a White House blog several years ago about a CISO complaining to Michael Daniel that, look, I spend millions for security that's regularly defeated by a $500 rented piece of malware. What is my extra investment in security going to yield? And if you can't put a number on that, I just don't want to keep throwing dollars into a pit and suffer a continuum of breaches anyway.

So I think actually what you're seeing is that there's acceptance within a lot of industries that breaches are going to happen, and that you're never going to be able to have 100 percent solution, so you're going to have to get to a high level of security but prepare for breaches anyway. And it becomes more of a risk management and a governance conversation.

MR. GORDON: Yeah, I don't disagree with what Matt said. I didn't mean to be cavalier about it, but take a look at the NIST 1.1 version. They explicitly say the tier you want to be on is a cost-

benefit decision. That's what I meant. It's, overall, you have to look at it from that point of view. So if you look at subsequent risk management, you need to look at it from a cost-benefit point of view. Even NIST puts it into their cybersecurity framework.

And NIST, when you talk about compliance, the NIST framework, ever since our current president said that all government agencies have to be at least consistent with that, that's been one of the biggest compliance issues I see, you know, to really get firms to look at their cybersecurity in a more serious way than they may have done in the past. But I agree. I mean, I didn't mean to be -- and not cavalier about it. I meant that they look at this as, you know, I can't have 100 percent security, so the question is how much do I invest.

MR. ROMANOSKY: So let me add one thing, though, that I think gets lost in the discussion and I don't think -- that I don't think is inconsistent with what both of you have said. But that if we're talking about firms and enterprises and enterprise-level risk management, cyber will just -- will be -- just one of the risks that they have to manage. And, so, yes, it becomes a cost-benefit decision, and I think that's

appropriate to the extent that we can reasonably quantify cost and benefits, and I'm not convinced that we need to, certainly as researchers anyway.

We really want data, and we love data, and we love analyzing data. That's kind of the fuel by which we go, but in this case, it's not clear to me that more numbers actually get us further ahead, but the real point is that if Cyber -- if we want to manage cyber, just like any other kind of enterprise risk, I think what we need to do is assume that if an appropriate assessment is done and it turns out that cyber risks don't pose that great of a threat to us, that they will be deprioritized, that the investments will be deprioritized. And I think we should accept that. That would be appropriate for a firm to do.

So when we speak of incentives, what doesn't appear here, so these are all incentives for firms who invest in cybersecurity. It doesn't really ask -- they don't really ask the question of how should firms prioritize cyber relative to all of the other risks they face -- tax and finance, employment, supply chain, competition. The list goes on and on.

So one useful exercise, I think, will be to understand how cyber relates in terms of risks to these other areas. And, again, if it's true that

cyber just doesn't present itself as a great risk, then it should be appropriately deprioritized.

MR. GORDON: Can I? I agree with what Sasha said, but I'd even go further and say that from an investment point of view, investments in cyber is just one of the major investments companies make. And companies, unless they're in business to sell cybersecurity, you know, services, they can't put all their money into cyber, so they have to look at this as -- they look at other investments.

And whether we like it or not, most major corporations use NPV models. They know they're not precise. It's a framework. It's a framework where they go through a process. And over time, you assume that, you know, the results from that process will be beneficial that year. You're going to have to make better decisions by following, you know, a set process, and I think when it comes to cyber investments, it's the same idea.

Cyber investments are competing with all other investments. I know lots of CFOs, and they tell me, well, everyone comes in and wants more money, they want a new product line, they want a new building, new equipment. So cyber investments are competing with other investments. And once you realize that, it's a

resource allocation decision for firms.

You know, for example, Target was spending a ton on cyber. It wasn't like they were not spending money on it. Their breach was due to outsourcing a little piece of their work, so I agree with what Sasha was saying, but I would just say it's more than just the incentives. It's across the whole level of investments, and that's the real issue. So you need a process, and the process has to be somehow consistent with the other investment decisions because eventually someone asks you, why should I give you more money rather than putting it over here.

MR. SHARP: So, Larry, I think Tyler brought up the point. It's about who bears the brunt of the outcome, the benefit of the outcome, and I think if we're thinking about this in the context of enforcement, which I think is a little bit the point, and thinking about if there is, in fact, an agency problem, meaning we make an investment that's appropriate for my firm but doesn't necessarily consider all of the externalities, then there's that true risk of market failure.

And I think that's the piece that while I agree there's a cost-benefit analysis and every CEO, CFO, CISO is balancing the allocation of scarce

resources fundamentally, the broader question is how do we effectively influence that for the protection of consumers. And I think we've circled around compliance.

Tyler, your research talks a lot about the compliance story, and I think in many cases it has helped related to, Larry, some of your research. The first dollar you invest in security is going to be much more effective than the tenth dollar you invest, meaning there are diminishing returns. And I think, Larry, your approach puts a cap on what is an appropriate ceiling. And, so, then compliance drives the floor, and somewhere in between I'm stuck negotiating with the various executives, and I think what we find that's maybe not represented here but all too true is there's an element of storytelling and charisma that CISOs bear the brunt of carrying in order to get the adequate budgets.

And if I can have an appealing story, and this sort of relates back to my original commentary, if I sit in front of my CFO and I can expand revenues, I get money. And if it is in front of that same executive team and I tell a story of the world is ending and no amount of investment will ever get me past the ifs, not if but when, then I can get money

once, and that's what happened in 2014 for a lot of CISOs. And then the money dried up by 2016, right?

MR. GORDON: Everything you said I agree 100 percent. So what I always talk about is revenue-generating projects versus cost-savings projects. And what Matt just said is exactly that point. So the example I always give is something like, you know, if you come and ask for a $10 million investment in a new product line that's going to generate $20 million in additional revenue, so let's just say the net benefit there would be the 20 minus the 10 or the bottom line goes up by 10 million, okay, you're much better off asking for that than if someone comes along like Matt and says, I want a $10 million in a network security, and I'm going to save you $20 million in costs, right, but you don't show any revenue growth.

And the name of the game for most senior executives, especially if they're on stock options, is revenue growth because the stock market -- there's lots of evidence, the stock market moves with revenue growth. So what Matt just said, I would say, can you come to my class? I talk about in this class all the time, exactly what you just said. And I actually bring in people like yourself, chief information security officers, to give examples of just what you

said, so thank you. I mean, that's a great testimonial.

MR. MOORE: Larry's class.

MS. JILLSON: Let's move now to talk about each of the incentives that's listed here. And, so, the first is customer trust, and we have a question from the audience about why we did not include customer welfare or customer well-being on this list of incentives.

So to what extent do you think that customer welfare, well-being, collapses into trust? And how much does trust matter? Does it matter if consumers begin to view a certain firm as no longer trustworthy on security, or do the number of breaches we've seen and the fact that people keep shopping at these places show that maybe trust doesn't matter that much?

On the other hand, does trust matter particularly in certain areas? So maybe for companies that have children's information, financial information, health information, you know, certain forms of sensitive data, where does trust matter, if at all?

MR. SHARP: I can offer the anecdotal evidence that comes out of CISO roundtable community discussions. Certainly for the discussions that we

have inside of the roundtables, the dialogue is basically customers have to trust in order for sales to go up, right? So I think we end up equating all of those things in a different way, whether it's competitive advantage or reputation or customer trust.

At the end of the day, protecting customers is important, but I think earlier in the session previously we've seen that consumers don't necessarily behave congruent with their own best interest. For example, the comment about 10 percent of Gmail users having multifactor enabled would lead to consumers just don't behave in a way that would be in their best interest because the email account is actually how you can reset every other password that they have access to.

MR. MOORE: So just the question about consumer welfare, I mean, I think consumer welfare is what, you know, when you're thinking about overall what the social welfare should be, then obviously you need to consider consumer welfare. When you're thinking about firms and what's going to drive their incentives to invest, their perspective is different. Their perspective is on what maximizes the firm's revenue.

If they're in a consumer-facing industry

where, you know, it's important that they respect privacy, it's important that they gain the trust of their customers, then they will act accordingly, but I think it's very much not the case across the board. You know, I mean, you look at the example of Equifax, which is, you know, that trust should be important to their business, but it was actually incidental. And to a certain degree, the trust that they needed to engender is with their customers, which weren't the people whose data was lost.

So, yeah, I think firms are going to, you know, in general, look at an incentive which is maximizing their own interests, which may or may not align with consumer welfare.

MR. LEGOWER: I want to jump in and move to discussion about compliance and liability. I think it's been brought up by most of you either explicitly or implicitly that you think that compliance and liability are big factors in cybersecurity investments. So the question I want to pose to the panel is, do these compliance considerations actually encourage more marginal investment or do they just sort of reallocate the investment that's already going to happen?

In a sense, is there just -- is it a hard

budget constraint on what you can spend and compliance considerations direct where it goes, or do compliance constraints actually spur additional investment?

MR. SHARP: Yes. I think it's both. It depends on the firm in that there are some firms who are maybe a bit more sophisticated and are thinking beyond just compliance, who have allocated their budget, and then they realize that there's a significant chunk of it that just has to be allocated to dealing with compliance circumstances, and that's the ideal, probably. But, then, there are other firms who otherwise would select below the floor. And the compliance requirements end up setting the floor, and that entirely directs what they need to spend their money on.

MR. GORDON: I think if they have a budget constraint and they can't go over it, then they're reallocating. And if they can get additional funds at the constraint, then it's a question of trying to figure out the sort of the best allocation. So it's a combination. It really does depend on exactly, you know, what Michael said was do they have a budget constraint, right?

And, also, the other point I would make is how are they allocating their funds currently. Are

they -- you know, compliance might force them to reassess their allocation process, or maybe they weren't at the best position from their point of view. They may reallocate it. So it's those two factors, you know, where are you in terms of the allocation of the resources and what kind of budget constraint do you have?

MS. JILLSON: Thinking about compliance and liability together, how is investment to ward off liability different from investing to meet compliance obligations?

MR. MOORE: At the most basic level, what their difference is is that you -- it's the ex ante versus ex post in the sense that, you know, you have a compliance rule in place because you want the investment to be made to prevent the harm from ever being realized in the first place.

And, so, if the harm is so great that it cannot be easily reversed or mitigated, then you focus on ex ante compliance. If the harms aren't so great, then you can just assign liability and deal with the fallout after the fact. When you think about breaches of personal information or any breach of confidential information, one of the big challenges is as soon as you have this breach of confidentiality, there's no

going back.

When all of the Social Security numbers get disclosed from a large data breach, there's no way to undo that breach of confidentiality, and so it's a one-way action. And, so, when you have situations like that where the bad event has sufficient cost and cannot be reversed, then the emphasis should be on compliance. If, in fact, the harms aren't so great or they can more easily be reversed, their effects, then you can push towards liability.

MR. SHARP: So, I'd love to respond to that. The dialogue in the cybersecurity community today has largely been we've invested, perhaps overinvested, in preventive controls in the network. And the reality is the conversations that are happening in boardrooms are about cyber resilience, acknowledging the "not if, but when" sort of paradigm of thinking. And I think you'll hear from some other very innovative firms that are starting to drive stronger opportunities to have more holistic prevention.

But when you look at the -- Sasha, I think it was you that made a comment earlier. When we're making decisions on where to invest money that we don't necessarily know what the best places to place those bets are, as CISOs, and I think there are some

nuances that we can pull out of that a little bit further and say, I think just about everybody that you would talk to in the security community would say we need to have multifactor, we need to have patching, we need to have configuration management, but every FBI and Secret Security briefing that you go to talks about how the overwhelming evidence is that patching is not functional and the configuration management is not working.

And, so, I think the question of we don't know what to invest in is not the real issue. It's we don't know how to make the organizational or process changes effectively in order to achieve the ultimate outcomes that we're after, and so I think there's nuance in the data that you're interpreting has a different nuanced outcome to consider.

MR. ROMANOSKY: I mean, I see those as the same thing. The point is we don't really know what's best. We don't know where to spend our first dollar. We have a list of -- we have a bucket of technologies, of processes, of things we think we should do. They probably all work to some extent, but we don't know where to start investing or to exhaust our budget.

MR. MOORE: And to your point about misconfigurations, we spend all this money on

controls, but we don't have the people in place to be able to adequately use them. I think that, at a high level, is still an issue of budget, right, because you need to be able to -- you can reallocate your resources to people who can be trained to be able to effectively use the controls that you have deployed. And there is definitely a challenge there because of workforce limitations and just the behavioral preference to buy another service or another tool rather than to adequately use the tool you have.

MR. SHARP: Yeah, I think the hamster on the wheel starts to become the issue. We get an unlimited number of vulnerabilities coming from the hundreds of thousands of users in different applications. And, so, no matter how good we do, there will always be a percentage of users that click on phishing. There will always be a percentage of applications that will not be patched, and so the dialogue -- and I think Matt probably can speak about this a little bit further -- is shifted to we're going to accept that some percentage of this can't be mitigated and we need to start to actively manage the downside impact through cyber-resilience investments.

MR. ROMANOSKY: I mean, for what it's worth, I really like that point. I think -- and, again, Matt

can speak of the insurance policies, right? So what you see in the applications and the rate schedules that carriers use is to ask a bunch of questions related to technical issues. There's some process stuff in there, but again we don't really know, right? We're asking a battery of questions that we think are correlated with better security posture, but we don't have any evidence to demonstrate which ones -- which technologies are better and even which questions to ask.

And I think I'm of the mind now that those nuances don't really matter and what does matter is the story of resilience and a maturity of processes. And I think the better we are able to assess maturity of processes, the more quickly we'll get at an understanding of better security posture versus weaker security posture, and resilience is tied into that.

And, so, I mean, I reject the claim earlier that there are two kinds of companies, those who have suffered a breach, those who don’t know it. I think that’s a silly comment, right? It’s a marketing comment. It just can’t factually be true.

But there is something to the point of, look, we should accept that we will be breached. And even if that doesn't happen, we should prepare for it.

And, so, what that means is that you establish a level of maturity of processes in order to maintain resilience. We accept that we start off with a level of output of our firm here, that we become resilient to absorb some percentage of that attack, of that outage, and that we develop processes to return to that 100 percent output level as quickly as possible. This is this resilience triangle that people talk about, and I think that's a smart way. I can't prove to you, but I believe that's a smart way of reducing the cost and addressing the problem.

MR. LEGOWER: So, I want to move on because we have -- since we have Matthew McCabe here and all this talk about resilience and risk management, I think we would be remiss if we didn't ask Matthew to talk a little bit about cyber insurance and explain how cyber insurers make decisions about which policies are appropriate for which companies.

MR. MCCABE: Sure. And I actually think it moves on just as a perfect segue from what we are talking about because I think that mind-set that you're talking about is what industry currently has. I mean, certainly, when we're going through an insurance process, the process is not a checklist of what technologies do you have and did you get seven

out of ten and therefore you scored a 70.

Quite frankly, the process is, you know, it might start with a question of how much data are you holding, what type of data are you holding, and what do you do to limit your sensitive data. And, then, there's the discussion back of what that process is of how you appreciate what your assets are. Do you really need all this data or do you have a data limitation policy?

So cyber insurance is all about the maturity of organizations. And, I mean, I guess I would reject the notion that it’s without basis of how to assess posture of a company. It is definitely not an exact science, but all reports are that the cyber insurance industry is profitable and, therefore, one could say that economically determined to be doing a good job for assessing security with -- you know, of course, there are breaches and there are claims and there are exceptions that pop up, but overall on a macro standard, doing very well.

So there’s -- I would say to really simplify the product of cyber insurance and maybe just to back up a step, it's different from having a cyber-related peril than having cyber insurance. Cyber insurance is a very specific product. Cyber-related peril means

that I was able to hack into an industrial control system, get something to blow up, and, as a result, there's a property claim or there's a liability claim. That's not cyber insurance. That's on more traditional lines like property or casualty.

For cyber insurance, you're looking at a bucket of three things. I've had a cyber incident, and I have to pay out of my pocket to respond to that incident somehow, whether in the data breach context that's providing notice and providing credit monitoring or credit restoration or whether that's dealing with a ransomware event and restoring data or replicating the actual servers or devices that have become corrupted, what's often called a bricking event.

Number two would be the liability angle, and I think that there's large amount of incentive that can be gained out of liability. We had the conversation between compliance and liability. I would look at compliance as a standard of liability. But if you can actually work with liability and find ways to cap liability by going above layers of compliance, then you have very powerful incentive for the private sector.

And then the third bucket for cyber

insurance really deals with the continuing operation of a company, what we would call business interruption. So if you're -- like in a NotPetya event if your company's been taken down and disabled, whatever extra expense you might have from that and whatever income that you've lost can be covered by the insurance.

But I will say for the product itself, as cyber risk has grown, the product and what it covers expands more and more every day. And I think that it's become -- look, the overall market for protective technologies in the United States alone is in the neighborhood of $115 billion according to Gartner Research. The overall amount of cyber insurance, global premium written, according to Betterley, is in the neighborhood of $5 billion.

So are those exact numbers? No, but they can give you a pretty good estimate of where we are from how much we've invested in protective security to coming on the scale of we're realizing it's really a management process. We're never going to be able to protect everything, so how resilient are organizations responding to cyber threats and recovering from them? And if you look at our industry, they have started to turn to the risk transfer part where the take-up of

cyber insurance has been in the neighborhood of 20 percent to 30 percent for four or five years now.

MS. JILLSON: So how should we think about cyber insurance? Is it properly thought of as an incentive to have better security because companies want better premiums and coverage, or should we think of it more in terms of it is simply a risk transfer mechanism? And is there a moral hazard problem with cyber insurance?

MR. MCCABE: So in reverse order, I would say no, there's not a moral hazard problem because I don't think that companies are spending on insurance in order to accept the fact that they have known defects. I think what they're doing is realizing that they can't spend their way out of this problem, and they're taking it on as another risk management strategy.

When the NIST framework was being developed, part of President Obama's executive order required three different agencies -- Commerce, Treasury, and the Department of Homeland Security -- to publish reports on incentives. And cyber insurance was the only one common to all three. And that seems like a very odd thing because it’s an expenditure. And you don't really view an expenditure as something to

incentivize better controls.

But I think in the mature sense, if you're thinking, look, if I'm going to have cyber insurance as part of my overall risk management strategy, then my ability to perform good security is going to be realized on the insurance side as well with declining premiums and with hopefully favorable terms. It's basically the investment of confidence by the underwriters. So I think that it's a function of leading companies in the right direction.

Look, if all cyber insurance did was transfer the risk financially, that would be valuable, but the truth is that it's helping companies to develop risk management response policies. It's helping companies assess their overall cyber posture. It's becoming ingrained in the whole cyber risk management approach throughout enterprises.

MR. MOORE: And I would just add, so to build onto some of your comments, I think -- I mean, fundamentally, there is risk transfer. That's a core part of the product, but there are these potential additional benefits that you can get, one of which is this idea that if you have someone -- an organization that comes to you and buys this risk transfer, then ideally they're thinking about the overall risk

management process. So that means they're already mitigating and spending significant amounts on mitigation and realize that they also want to do some transfer as well.

There's also this fact that the insurers go through this process of evaluating clients and ensuring that you are spending enough on mitigation. So if you want to get a reduced premium, then you need to take certain steps and show that you've taken it, so that's definitely a benefit.

In terms of the moral hazard question, I would say it's not really a concern now. In particular because most companies cannot fully insure the potentially unbounded scope of what a cyber insurance loss could be. Frequently, companies say that -- large companies are not able to necessarily even buy as much coverage as they might even want to, and so there are still relatively low caps on the amount of coverage you can get. And so, worst-case events go way beyond what tend to be covered, so that's one thing.

The final point I'll make is that the existence of data breach notification obligations through these state laws has really helped bootstrap the cyber insurance market for reimbursing costs

surrounding data breach. So, you know, and the fact that there is this obligation to disclose creates the obligation for companies to have these costs and then make them go ahead and apply for -- get insurance and file claims.

Other forms of cyber insurance -- or other forms of cybersecurity and cybersecurity risk, there's still a calculation as to whether or not you'd necessarily even want to file a claim with your insurer because you might then have to publicly report it. And so that's an example of the policy intervention of data breach notification enabling cyber insurance.

MR. ROMANOSKY: Can I ask? So, Matt, you made one comment that was curious. You said -- tell me if this is wrong. Insurance companies are profitable, therefore, we are able -- that shows that we are able to properly assess risk.

MR. MCCABE: It shows that these companies who have been writing cyber risks for 10 to 15 years and making profits on it are doing their business well.

MR. ROMANOSKY: I guess that's the part I don't understand. So the more profitable the company is, the better it shows that they're able to assess

the risk. So the profitability comes from having premiums, issuing premiums but suffering no claims. Right, if there are no claims, then the firms -- the carriers can be most profitable.

MR. MCCABE: Oh, no. They have claims. What they're trying to do is assemble a portfolio of diverse companies.

MR. ROMANOSKY: Oh, I see.

MR. MCCABE: They're trying to -- well, I mean, we can go back to 101 and explain the insurance industry, but there's undoubtedly the profitability of an insurance company in writing cyber portfolios is testament to how well the job they're doing.

MR. ROMANOSKY: But that profitability comes from diversification of the portfolio as opposed to being able to better -- as opposed to being perfectly able to assess the cyber risk.

MR. MCCABE: There's no perfectly to anything in the world. Government decisions are never made in a continuum of perfection. Educational decisions are never made in a continuum of perfection. Economic models are never drawn up in a continuum of perfection. What there is is an assessment of what maturity of organizations are. And it's not just diversification. It's an evaluation of security

posture.

If an insurance company spots a potential insured that has flagrant weaknesses and a lot of exposure, the market will recoil. And as a result, the prices for premium of that company will go up. And to your point, the amount of limits out there for that company will be less. I think that is a completely appropriate market response for cyber assessment.

MR. SHARP: Can I just -- let's say you have -- and this is a common thing -- a billion-dollar company, 3 percent of revenue spent in IT and 10 percent of that being spent in cybersecurity. So a billion-dollar company could be spending $3 million a year in a security program. That company may choose to insure to protect against a breach of something like 5 or 10 million records. That policy would cost somewhere between $30,000 and $60,000.

Let's say that you double it. Let’s say that you triple it. If it’s $150,000, the incentive to me or to my team to really build a $3 million program in order to reduce $50,000 off of my insurance doesn't make sense. So I find some -- so my personal experience -- and this could be an anomaly -- is that's not a dialogue point in any of the discussions

that I'm having with any of my peers nor with my executive team.

And then the other thing that I would offer is -- and I don't know that your firm -- your firm may operate differently, but I've been in a couple of rounds of purchasing this cyber insurance, and the brokers come in and they bring a group of folks to ask some questions. And, categorically, the questions are insufficient to tell really what's happening, so it seems or it would appear, if I'm extrapolating, that we're doing assessments similar to demographic assessments in like car insurance where you say -- you look and behave in a particular way.

You're 20 years old. You're a male. You live in this area code. And, therefore, we're going to classify or price this policy in a particular way, which is different than the more informed version of plug this thing into your car and we'll measure your accelerations and decelerations and the way that you actually behave on the road.

And, so, it looks like the questions that are asked are more targeted towards mitigating or adequately litigating, not paying an insurance claim. And it looks like the instruments that we have to measure cyber liability are dramatically insufficient,

just from -- that's my perspective, and I know that that could be different than your perspective.

MR. MCCABE: Well, the instrument to measure cyber liability has got to be data on what's been paid out before. And we are certainly at nascent days of the standard of care. Now, as far as coming in and asking what those questions are, one of the things that we should be aware is that there are more and more tools that are becoming available to underwriters to actually assess risk, but you're right, unless you're within the footprint and doing a forensic assessment, you're not really going to know what's going on.

But the fact is that from a macro standpoint, are they looking at different sectors and companies within that sector and being able to judge them one over another from the survey they get, the questions for followup, some kind of external data analysis? You get a decent picture for the purposes of insurance. Now, is that going to stop cyber attacks? No, but we're not stopping cyber attacks. We're managing cyber risk. We're helping industries become more resilient.

MR. GORDON: Can I say one --

MR. LEGOWER: In the interest of time, I

think we have to move on, but you'll be happy to know that we're going to hand the mic to you. So we're going to turn now to the mechanics of how companies actually make decisions about investing in security. And to start us off, I'm going to ask Larry to explain the model that you've developed for cybersecurity investments.

MR. GORDON: So you want me to click this?

MR. LEGOWER: You've got your slides here. Yeah, there you go.

MR. GORDON: Oh, okay. So I think of this as a framework. I'm not lost in the mathematics. There's a lot of mathematics that underlies it. So the framework is very simple. It's a process where you look at -- I think it was Matt who mentioned with the cyber insurance that you look at companies, you want to know what data you're trying to take care of, what's the value of it.

So the first thing you want to do is figure out what data you're trying to protect, what's the value of it, and the value of it is in terms of how much could you lose, you know, the cost to you. So that's part of the value.

Okay, and then the other thing is what's the probability of a breach. And then, lastly, is how

effective are your investments, the productivity of investments. So it's three very simple aspects to the process. One is, you know, what's the value of the information you're trying to protect, what's the probability of having a breach, and what's the productivity of the investment.

And, so, without going through mathematics, you look at those three things. You can develop a grid like you see in the middle. They have the chart. The chart on your left-hand side, all it's basically saying is exactly -- I think it was Matt or somebody else mentioned that if you put more money into investments, the first dollar you get more out of it than you get the second, so the value of the investment is -- the benefits are increasing at a decreasing rate. And that's really all the left-hand chart says, but it also says there's an optimal amount to invest. I don't know the optimal amount. It would change for every company.

And no matter what you think, it is ex ante, ex post, it's probably not going to be the right amount, but what I would argue is following some sort of a rigorous process over time, taking into consideration what the others here on the panel were saying, that resilience and looking at what I consider

control, seeing how you did at the end of the period, so you make these decisions ex ante and ex post. You evaluate it, and then you move into the next phase, so it's a continuous feedback process, and that's the intent.

The nice thing about that middle grid there is to suggest that you could come up with a grid and look at how much you think you might want to invest in different databases. I'm a big believer in segmenting databases. So you can look at how much to invest in databases, but the nice thing about it is you can do a simulation around it. So you don't like my probabilities that I threw in? Throw in a whole bunch of your own and do a probability assessment.

You could also -- you know, the value of the information, no one knows exactly the value in terms of what you're trying to protect and what you could lose, but you could do a simulation around that. So that's the whole idea.

The last little picture on the right-hand side, all that's saying is that it started off as an academic model. It was originally published in a computer science journal with a lot of mathematics. And eventually I kept saying to my coauthor, Marty

Loeb, and actually one of the other papers we wrote, Joe Lay (phonetic) who's actually sitting in the audience, we actually came up with an example, and we tried to show how to use the process.

And to my surprise, the Better Business Bureau picked it up and actually put it in a 2017 report and recommended it to all small businesses in North America to think in terms of this framework. Again, not using -- you know, not getting caught up in the actual numbers, per se, but it's a process that you go through and you figure out, you know, the value of your information, the probability of a breach, and what do you get for additional investment, so what's the productivity of investments. And, so, that's all that slide shows.

MR. LEGOWER: I think you had another slide.

MR. GORDON: I have another slide. I can just -- you know, I've actually -- you know, it's something Michael asked about. This one was about incentives and government incentives. And it really got to the issue of, you know, what can the Government do in terms of giving incentives. Most incentives that were in the slide that Elisa had before were really things from the firm's point of view.

So the Government's been looking at lots of

incentives. You know, they give tax incentives, grants and so on, but it's not that obvious that giving incentives, okay, will increase security. One of the problems is we don't really have a clean measure of security. So all this little slide is supposed to show is that you can show very easily that the Government -- if a firm was already allocating their funds in an optimal manner, then government incentives, which would shift their allocation if they have a budget constraint -- Michael's point -- would shift it away from a better solution.

On the other hand, if they can increase their budget, then government incentives would tend to increase the level of security, so that's the bottom line of what's on there. That was -- actually, I should mention that the first -- can I go back on that?

MR. LEGOWER: Oh, yeah, go ahead.

MR. GORDON: Yeah, how do I go back?

MR. LEGOWER: The red button.

MR. GORDON: This one?

MR. LEGOWER: Yeah.

MR. GORDON: Okay, so I should mention, the model, when we originally developed it, we were being supported by NSA. And -- going forward -- that's

okay.

And DHS actually was very interested in what kind of incentives we could give to the private sector as a Government, you know, to increase security, and so we looked at some of the issues. And this was one of the things that we talked about in our report.

But there's no absolute. I'm not lost in the mathematics. I think the mathematics gives you insight, and then, actually, you know, looking at a process.

MR. LEGOWER: So, I want to follow up. So, you know, the first picture here, the declining function -- or, sorry, the function that's increasing at a decreasing rate, that's the productivity of investments.

MR. GORDON: Right.

MR. LEGOWER: So, I think Sasha was alluding to this earlier, that, like, nobody really knows the shape of that function to some extent, right? And it's a big component of, you know, where the optimal point on that curve is, is what that curve looks like. So does anybody -- Larry, you can start us off, but does anybody have ideas on, like, how we can maybe go about estimating what that curve looks like?

MR. GORDON: So we originally -- what we

looked at was different -- we called them security breach functions, so we looked at different productivity functions of investments, okay? And based on a couple of broad classes of investment productivity functions, we were able to show that there is an optimal level, and it's much less than a lot of people think. It's, you know, roughly one-third of the expected loss. Mathematicians around the world started to say this is nonsense. I got emails saying this is voodoo economics, and then eventually a mathematician in Russia and one in France around the same time said these guys stumbled on something that's more powerful than even they realized. He was right for me but not my colleague. He knew it was right. Okay?

So Marty Loeb, who's not here, I went to Marty, and said, maybe the guy's right. These were math professors, and he says -- and we did look at different productivity functions, but you can find some that it doesn't work. All that graph is intended to show is there's diminishing larger returns to levels of investments. You know, you put in -- you know, if you look at your opportunities, you should be able to get more for the first million than for the second million, whatever investing in. If it's a

smaller company, more for the first 10,000 than you'd get for the next 10,000.

And, so, ever since the Better Business Bureau came out and recommended the framework -- again, they recommend the framework. They don't say get lost in the mathematics. I've had lots of small companies come and talk to me, and I talk about the framework. You know, it's a process. You're better off to use some formal process than just, you know, ad hoc, poof, some number out of the air. And you're never going to get them right, and one big breach and the whole thing falls apart.

MR. SHARP: So, the folks with Rich Seierson and Doug Hubbard did some additional research that I think complements and maybe contradicts in some places, but what they were able to do is start from the foundation that there is a way to make calibrated predictions about things that we can't measure today or have been unsuccessful because we don't have the adequate information to measure today.

And I think the other thing that they highlighted was that there's some false thinking out there stemming from statistical illiteracy around how much data you need to come up with functional models. But at the end of the day, what is true is using

calibrated assessments with folks who have expert judgment, you can get fairly accurate estimates of probability. And I think using that information with a properly calibrated expert you can actually get fairly accurate estimates.

But to -- I forget was it Sasha or you, Tyler, the validation that this is, in fact, the appropriate curve or this is the best model, I don't think we have empirical evidence to support that part, right?

MR. GORDON: I agree completely. So I should just tell you, we had a consulting firm in D.C. -- I won't mention the name -- said, let's take your model and we'll go to all of our clients, and we'll bill you out at a high rate and you'll get a great consulting fee. My response was, what, are you crazy? Any number we give them is not going to be the right number, but you're better off to go through a process. Let them try -- each firm is different, and exactly what Matt said, with the right experts in the firm, they can -- it's better than just pulling numbers out of the air.

And over time, I would argue, the same way I would argue for net present value models, I would argue that they're better off doing it that way than

just ad hoc be pulling numbers out. And I think, you know, what our other Matt said was that even the insurance companies, you look at what kind of information you're trying to protect, what is it you're doing. You know, and so it's a formal process.

And, so, even though you may have thought I'm going to come in here and try to sell you on the mathematics, I'm not. You know, I understand -- there is some real mathematics underlying this.

MR. MOORE: And I think in some sense the question is, like, you know, the question may have been, you know, how can we collect data to maybe, you know, best validate what this model is. I think maybe that's not the right question. I think the real problem that we face is that we don't have data on effectiveness of controls, right?

And, so, we maybe have some point estimates of the likelihood of different categories of security events like breaches and how they could vary by sector, but what we have very little insight right now onto is how effective these particular security controls are or even this class of security controls are against these kinds of threats. And if you were to increase your investment in this control or across these suites of controls, how would that reduce your

expected losses? And we just have no idea.

Okay, I think I've been provocative enough to elicit a disagreement, but the -- I would argue we don't think we have a good sense of what the -- you know, what the true cost of an attack is and, more importantly, how effective certain defensive countermeasures are. And I think part of the reason why is I think there is just not a lot of interest among the vendors and designers in the cybersecurity industry in providing this. And it's hard to do. I think it's very hard to do, but it's also not something that they're interested in providing, and so I think fundamentally that's something that we need to make more progress on if we're going to get more effective security investment. Now Sasha?

MR. ROMANOSKY: Yeah, so, yeah, that's true. So I was initially -- I probably sounded very critical of the insurance industry, and I don't mean to be. I probably was when I initially started doing some of this research, that, you know, oh, my God, we all turn to insurance companies because we think that they should have the perfect answers for everything and they should be these wonderful seers that can provide perfect investments.

And, so, I started looking at these rate

schedules and saw that, look, this is not quite great. But the reality is that even I wouldn't know how to do a completely accurate assessment, right? I can give you a good idea of what to look for, but even I wouldn't be able to do that. And I think they're trying, right? So, you know, you can see the evolution of these policies evolving over time, and I think that's a good thing.

I do think that they provide the only opportunity to get at exactly the kind of data that we really want, right, exactly the kind of answers that we want to understand, which is what kinds of security controls matter and by how much. And they have that through the claims data. And this isn't rocket science, right? All this takes is a little bit of statistics, a bit of a regression.

So you can imagine in your head a spreadsheet, where all of the rows represent the cyber policies that a carrier has or a group of carriers have, right, so every policy. The columns -- the first column represents whether or not a claim has been filed, yes or no, say in the past 12 months. And all of the other columns represent properties of those firms, the industry, the size, number of employees, and then answers to the security questionnaires, what

kinds of controls they actually had.

And you just run a regression, and you get an answer. And maybe it’s not a perfect answer. Maybe you don’t -- maybe not everything is statistically significant, but you start to get at a sense of here are the kinds of processes, procedures, security controls, whatever, that actually matter and then predict in a statistical way of affecting whether or not a breach occurs and a claim has been filed. Right? That's it. It's nothing more sophisticated than that.

Yes, there are issues with data and data cleaning, and do we have the right kinds of questions and whatever, but that is one way -- that is the only way that I know of to be able to get at a way to validate this model and get at very useful kinds of questions.

MR. SHARP: And I would just say there may be some sampling bias. Having worked at a couple of firms and actively participated in a process of helping companies respond to data breaches and other kinds of security compromises, I think it's very rare that those data breaches actually get publicly disclosed, so I would say, you know, fewer than 2 or 3 percent, if I had to put a number on it.

And, so, I think the information that we do have that would come out of the insurance folks should be properly caveated to take into account that there's a set of drivers that cause people to disclose and not all data compromises or security incidents or what have you are effectively represented in the data that the insurance companies have.

MR. ROMANOSKY: Dude, my research is full of caveats. I have no problem with caveats. But that doesn't mean it can't be done.

MR. SHARP: Sure.

MR. ROMANOSKY: That we can't try.

MR. SHARP: Yeah.

MS. JILLSON: So firms are reporting that they are spending more money on cybersecurity. Do you think that even if we don't know necessarily what controls are the best in particular instances if we don't have that kind of data, can we look at kind of overall spend to get a rough sense as to the security at an organization?

If you're coming -- if you’re looking at it from a regulator’s perspective or if you're coming into an organization as new security personnel or on a consulting gig, can you look at that rough spend and get some sense as to likely security?

MR. GORDON: If you had the number, that would be great. The problem is firms don't report how much they spend on cybersecurity. I've got about ten studies. I'm sure everyone else who does research in the area has about ten studies waiting to go if they had that kind of a number. In fact, I actually -- when I testified in Congress, I actually said one of the things that would be great if we could have is somehow have firms report how much they actually invest in cybersecurity.

MR. MCCABE: It's a really common metric for when you're applying for cyber insurance, how much, but it's also very difficult to ascertain because it's not necessarily a clean budget item. You have cyber investment in a lot of different disciplines.

MR. GORDON: They're giving you private data. That's not publicly available.

MR. MCCABE: No, it's confidential.

MR. GORDON: Yeah, that's what I mean. It's hard to --

MR. MCCABE: Yeah, it's not in their 10-K.

MR. GORDON: Yeah, right. That's what I meant.

MR. MOORE: I mean, there's definitely going to be correlation. I think that -- I think

the correlation is going to be very noisy. And, furthermore, because we have these problems about information asymmetries, about the quality of investments, we have these systematic -- systemic problems that will make it very, very noisy. That's what I'd say.

MR. SHARP: So there are some sources of data like Gartner and Forrester and IANS and other folks who do aggregate benchmark data and then share that functional data. I mean, it’s a part of every CISO's pitch deck for whether you’re getting more or less funding. You include it when it helps you and you don't when it doesn't.

MS. JILLSON: All right, let's turn now to another slide. So this is a polling question, so I’d like to ask this question to the panel. So who provides or should provide incentives to invest in data security? And to a certain extent, this overlaps with where we started our discussion.

So A, culture, which could be security professionals, executives, or boards.

B, customers or consumers.

C, cyber insurance.

D, law, whether the source of that is state statute, state of breach litigation, federal agencies.

Or E, other. Or you can choose some combination thereof.

So let's run down the panel and hear each of your answers. And let's do the reverse from last time, so let's start with Larry.

MR. GORDON: It's simple. A through D and probably add E, also. You can come up -- you know, there's no one incentive. That’s what -- you know, we started off with incentives. There's no one incentive. I know one thing, the SEC certainly has now become very interested in cybersecurity risk, starting in 2011 when they came out with their disclosure guidance from the Corporate Finance Division; then in 2018, when the Commission came out with a statement on cybersecurity risk and then in 2018, on top of that, when the Enforcement Division came out with internal controls, accounting internal controls should take into consideration email breaches. And I think these are all incentives. And I think every one you got listed there, as I look at them, you know, you can pick one, but I think they're all important. I think they're all important. I'm copping out on you, but I really -- I believe that.

MR. MCCABE: Yeah, for D, I don't really look at things like litigation and mandated compliance

regimes as an incentive. I view that as the other side of the coin. An incentive should really be about, okay, other than meeting my bare minimum compliance requirements, what are my interests in going above that model? And there's a lot of ways to achieve it, as Larry said. I mean, I think what you really do it for is A and B. You do it for your corporate reputation, and you do it to make sure that you have customer trust and that you're going to have that good faith and that good name, but I think that there's a lot of mechanisms in which the Government can participate to provide incentives.

I would give as an example from the terrorism world the Department of Homeland Security's Safety Act, which gives litigation protections for companies that are able to demonstrate that they have security that is more likely than not to deter a terrorist incident. You can apply for Safety Act protection. Things like that I would consider more of an incentive rather than the Luca Brodsky incentive of you've got to do this.

MR. MOORE: Okay, I will do a variation on what Larry said, and I'll give you a rank ordering. So I think ideally it would come from the customers and consumers. And in the cases when you can get

that, when the consumer demands sort of naturally align, let's go with that, that's great.

It doesn't always work out. And when it doesn't work out, you better hope that the companies themselves have a culture to make the right investments and to do the right thing. And if that doesn't -- and one of the ways in which that could be magnified is through cyber insurance in that it can provide sort of an outside perspective to sort of validate what you're doing and also provide some sense of, you know, what the true cost of insurable events are, so that sort of can magnify, you know, a company whose culture is already in the right place.

But, then, I think the last step has to be the law, and I think because you're not going to get complete coverage from just those first three because of the presence of the market failures I talked about earlier.

And in terms of what the law can do, I think the law can do steps to remedy those actions. In particular, try to mitigate the information asymmetries by collecting and disseminating data that would enable us to evaluate security controls more effectively, for example, by having increased disclosure about cybersecurity risks, some of which

we're already seeing through the SEC guidance, as Larry alluded to.

You know, litigation, as a stick, in the event of companies that just are not acting in good faith. And, so, that's the order in which I would put it. I think you need them all. There you go.

MR. LEGOWER: That's kind of interesting. It seems like you're implying that the law should sort of act as a force multiplier for the first three. It's like you should give information to consumers so that consumers can direct incentives. You should, you know, impose liability so that cyber insurance has teeth and things like that.

MR. MOORE: Absolutely. I'm a believer in capitalism. I think, you know, when you have to have government intervention, it needs to be in order to make private markets work better.

MR. ROMANOSKY: Yeah. So I think D starts -- provides the floor, right? It's a compliance, the statutes, the enforcement actions, it provides the floor, and then comes from customers. So to the extent the customers actually care about firm behavior, they have an opportunity to drive things. I don't see that happening, right?

We had a discussion earlier about the extent

to which firms invest and respond to -- whether or not firms compete on privacy and security. And I don't think investment in different kinds of technologies provides you that answer, and I don't really see that much of a market for it anyway. It's an old problem, and we've talked about it a lot, but I don't see it changing.

I think the firm -- the board -- I don't see much of an impact from A, right? The board's going to respond to costs and different threats, and those costs are going to come from consumer behaviors. And, again, if the consumer behavior isn't there, if, like, that pressure isn't there, they're not going to respond.

And the same with cyber insurance. Right now, you know, I just don't see it as having a great opportunity for driving incentives.

MR. SHARP: Yeah, I'm remarkably aligned with what Sasha shared. The law and the compliance is driving the floor. And for those folks that are looking to be checking the box, that helps pull them back into reality and do the right thing, but for those folks that have come to the conclusion that cyber resilience makes sense, then you have a combination of customer demand in a culture that's

driving the story forward. And I think that cyber insurance is a part of an overall risk management strategy, but I don't see that as an incentive, frankly, at all.

I think when you think about drawing up the laws, it's important to consider we have organizations with varied business models. That means different margins and ability to invest in things. And we also have a different size and scale of organizations, and so, not that this is news to you guys, but what that means is that you have an entire set of “check the box” customers that we encountered in my consulting days quite frequently that would benefit a lot from increasing the floor.

And then I think what you find on the top end is compliance can be disruptive and redirect investments in unhealthy ways. So for example, we help people move to the cloud. When people are in the cloud, the technology behaves very differently, but the rules and the compliance standards are written in ways that make us have to jump through additional hoops in order to solve things in ineffective ways when we can get stronger security outcomes using new technology paradigms, so I just would also put that on the docket.

Compliance certainly does, for those more innovative and secure firms, actually create a drag, and that's an unfortunate reality.

MS. JILLSON: I want to thank all of the panelists for their time and their insights. We are now going to take a 15-minute break. We'll start back here at 2:45 with a panel discussion of consumer demand for security.

(Applause.)

(Recess.)

CONSUMER DEMAND FOR DATA SECURITY

MR. HO: Okay, good afternoon, everyone, and welcome back to the third session of the day on the consumer demand for security. Again, my name is Jared Ho, and I'm an attorney in the Division of Privacy and Identity Protection. I'm joined by Mark Luppino, an economist in our Bureau of Economics.

We'll start out this session today first with a presentation from Justin Brookman from Consumer Reports on the standards that Consumer Reports uses to evaluate security.

Then we'll kick it off to a moderated portion of our panel with a polling question. As with previous panels in the morning, there will be event staff walking around with question cards. If you have a question, please flag one of them down. They will collect the cards and pass them up for us to read.

And with that, do you want to give introductions?

MR. LUPPINO: Sure. I'll briefly introduce our panelists. To my left we have Justin Brookman, who is the Director of Consumer Privacy and Technology Policy for Consumer Reports Advocacy.

Michael Higgins is a 30-year veteran of the information security industry and has previously

served as the CISO for NBC Universal, The New York Times, and LexisNexis.

Wiley Hodges is a Director in Product Marketing in Apple.

Kirsten Martin is an Associate Professor of Strategic Management and Public Policy at George Washington University School of Business.

And Rick Wash is an Associate Professor at Michigan State University in the Department of Media and Information, where he codirects the Behavioral Information and Technology Lab.

With that, I will turn it over to Justin.

MR. BROOKMAN: Thanks. Can I have the clicker?

Thank you. So I was asked to give a little presentation on what we're doing at Consumer Reports around demand for security. So, first, just a couple words about Consumer Reports in general. I think most of you all know we test lots of stuff, right? We have 8 million members now, test about 7,000 products a year. I think generally we're recognized as independent and expert and data-driven in the advice and information we make available to folks.

A few years ago, though, I think we started to recognize that we really weren't capturing all the

elements, all the lot of modern products, especially connected in smart products. So we started to think about how can we start to do tests and evaluate products and services for things like privacy, for things like security, for things like ownership, right? Do we even own our products anymore? Do we have the right to resell them, the right to repair them? Things like interoperability. I have a bunch of smart things in my house. Will they talk to each other? How do you give and evaluate points to products based on that sort of thing.

And, so, the Digital Standards, a project we launched a couple of years ago, originally Consumer Reports sitting down with some partner organizations, ranking digital rights, who's part of New America, the Cyber Independent Testing Lab, and Disconnect Me makes privacy tools like the Disconnect ad blocker, and started to think, okay, if we're going to evaluate products based on privacy and security, what are the criteria, what are the elements that we're going to look for.

And, so, we published this document online. It's available if you search for the digital standard. It articulates things like, you know, product support over time, control of your information, what do the

policies say. It's an open-source document. It's available on GitHub. We're constantly reevaluating it and looking at it and tweaking it. I'm going to spend some time in the document on Friday, making some suggestions based on some of the testing we've done so far. So if you have ideas and you want to take a look and think about some of the things that we suggest and make some suggestions for refinement, we would certainly appreciate that.

And, so, I wanted to talk just a little bit about some of the actual elements in the standard for things that we look at on data security. So use of encryption, is data transmitted encrypted on the device, is it encrypted in transit? Ideally, we would look to see if it's encrypted in the cloud server side, but that's hard for us to evaluate.

Commitment to support periods, a really important thing for us. Right now, there's not a lot of information available to folks about how long. If I buy a smart TV, will it be supported for 5 years, 10 years, 20 years, 1 year, no year. Not a lot of information available about that.

When I was here at the Federal Trade Commission a couple of years ago, we did a report on smart phones, how long smart phones are supported for.

Found just a vast, wide range of practices, right? Some super expensive flagship phones just didn't get any support, were vulnerable to attack straight out of the box. Some phones got supported for, like, years and years and years. Right now, not a lot of information for folks about that.

Resistance to attacks, there are certain penetration tests we can do in our labs about things to see if things are vulnerable to certain common types of attacks, and can we do that ideally without violating the Digital Millennium Copyright Acts?

Passwords, again, obviously the passwords should not be passworded out of the box, but do they support long passwords, do they allow cut-and-paste from password managers, do they have a bug bounty program, so they allow/encourage third-party researchers to come and say, hey, we found this problem on your site, a process for taking those sorts of things into account.

Security oversight, do they have a security oversight program? Again, hard for us to test. We may not be able to have a lot of visibility into that, but there may be some indicia we could look at as representing that they have with a program in place. Do the updates happen automatically? Even if a

product is supported, it's not going to do a user a lot of good if my router software is available on Router.com but doesn't come to my device, maybe give credit for automatic updates that are pushed to the device.

On the other hand, what if they're bundled with functionality updates as well? There is recently criticism of Epson for bundling security updates with updates that actually impinged upon someone's use of the products, so how do we consider that? Multifactor authentication, something that can in some cases be useful for security.

Best build practices, is the product not overly complicated, is it not overly reliant on third-party code and libraries, which might introduce some fragility into the system? Are folks told about changes if my password's changed, will I be told about it by email or some other service?

And, then, are updates authenticated, is it actually authenticated from coming from the server or from the manufacturer? This is just a handful of them that I thought it would be useful to kind of, like, walk through what we're thinking. There are more on the site and that we're trying to operationalize in some of our testing.

And, so, the goals of this should be obvious. Right now, there's not a lot of information readily available to folks in the marketplace about privacy and security practices, so if folks do want to make security-conscious choices, this will empower them to do so.

At least as important is kind of pushing the supply aside as well. Right now, I think a lot of companies don't have accountability for dodgy practices. They kind of skate by on ignorance of folks knowing what's going on. If we give a company a low rating, they get mad at us. They take these things seriously. They'll call us and complain and occasionally sue us. So if we can introduce some degree of accountability for practices that -- I think we've all seen in the security space a lot of, like, common practices are actually just things that could easily be remedied.

Certainly a lot of FTC's data security practices are things that really should have been captured but somehow they just skated by on. I think the Equifax security breach, which was reported on in the Senate oversight hearing the other day showed things again that really should have captured from the beginning. If we can push folks on the supply side to

think more about these things in advance, I think that's good for the ecosystem.

And, so, I'm going to walk through a couple slides about, you know, how we've been doing this, how we've been kind of like building out our program, originally just looking at kind of -- occasionally things like apps, like so investigative journalism type things. Here's an app we looked at called Glow, which is a woman's fertility app. It has access to super-sensitive information about folks, and we dove into it and found, like, a lot of sort of security vulnerabilities. Again, things that could have easily been addressed. Passwords could have been changed by attackers. Attackers could get access to pretty sensitive stuff without being authenticated.

In this case, we did responsible disclosure, went to the app manufacturers, explained at length all of our findings and concerns, and before we published, we got them to address them. But this is how we first started thinking about how do we apply the digital standard in practice.

Then, last year, we did an expose on some smart TVs on data security and privacy. On security again, we didn't see any of these companies promising to update software, provide security support for any

period of time. So consumers had to kind of go in hoping and guessing.

We found a couple of security vulnerabilities in the Samsung and Roku TVs. Attackers would be able to change channels and put on objectionable content and put the volume to 99. Again, more nuisance type stuff, but things that probably should not be possible to be done. I know at least in the case of Samsung, they agreed and did actually update their software to address the concerns.

On the privacy side, just recently I worked on a -- at the Federal Trade Commission as well, a lot of smart TVs have the capacity to watch what you're watching, so they will take snippets of what you're watching and send it back to the lab, and then they can kind of build out a pretty dense behavioral profile about all the things that you do on your television.

I think because of the FTC's work on the Vizio case, they all kind of asked for permission, they all push you through some screen where you had to press okay. Varying ways of doing that, varying degrees of how good that was. Again, from Consumer Reports' perspective, you know, how do we evaluate

user design like this, how do we give points for how big the okay is and where the skip or don't or say no button is. So definitely a concern for us about how to evaluate on privacy, but also for security choices as well.

And, now, more recently we started to actually translate these into Consumer Reports ratings. So this is one from a couple of months ago. We looked at some mobile peer-to-peer payment services. Fortunately, to avoid any awkwardness in this panel, Apple ended up doing quite well in this evaluation. You can see we look at things like we might look at otherwise like authentication, is there customer support. Do folks -- but then two of the five categories that we have are also on data privacy and data security.

And ApplePay is actually very thoughtfully designed to actually limit the amount of information that Apple itself ever collects by any transaction to limit the way that any information could be used for identity theft in the future. So in this case, Apple did really quite well on both privacy and security.

The other companies, you know, getting in. It's hard to test, right? I mean, the information could be sold or leaked or used on the back end

without a lot of visibility. And to us, we had to rely in large part on the disclosures they make, and some of the companies reserve pretty broad rights to do lots of stuff with your personal information. So in this case, they ended up scoring not as well. And these were things that were incorporated in the overall score.

Some of the challenges that we're confronting so far. So, one, we actually have to rely on documentation in a lot of cases, and it's often not really illuminating. You all have looked at privacy policies. Privacy policies today are not really designed to convey meaningful information to folks. They are compliance documents that are designed to evade liability. So if you're actually trying to look at what companies are doing on privacy, it's actually hard to tell. Even if you had the time, like I do, to review privacy policies for a living, it's hard to get a lot of information about it.

Right now, we don't have a lot of information about how long products are being supported, like I said. I think we'd like to build that out over time if, in fact, Samsung washing machines get updated longer than others. Would you want to be able to say that? That could go into some

sort of reliability type metric that could be incorporated into ratings overall.

Right now, we don't have that. Right now, there's not a lot of ground troop we can point to. Even trying to go back in time and try to figure out how long the products have been supported is actually quite challenging but something that we're committed trying to figure out. Some things it's really tough to test. You know, do we have to compile every software system? I mean, even if we could, it's actually quite challenging and expensive to do that, and then there are lots of things we can't, like, again, anything server side, we don't have any insight into. There, we have to rely on the documentation. Like I said, there's not enough information that we would like.

And, then, you know, how you translate a set of tests to a constantly evolving set of product buckets. You know, products are different. They may have different threat models. They have access to different types of information, so access -- you know, information on the phone is very different than on a smart TV. And, so, how do you do that sort of changing and testing at scale?

You know, scores are going to be subjective.

You know, we try to make them as objective and repeatable as possible, but you're going to, you know, identify 12 out of a handful of criteria that we're trying to compress into a fairly narrow set of information, and how do you do that reliably and fairly?

How do you give points for vulnerabilities that they actually patched? Like the example of Glow, we looked at like -- we found, like, a bunch of different vulnerabilities. And, so, if the company says, okay, we patched them all, give us a perfect score, like how do you take into account what may have changed? And, like -- and things change overnight, right? I mean, a software update can change everything radically. It might not even be a software update. It could just be some interface change. It could be a policy change; it could be a practice change that we don't have any way to check for.

And, so, how do you -- again, if you're testing 7,000 products, not all of which are connected but more and more are, how do you set up systems to keep track of them over time and to make sure the scores are accurate.

And then, you know, just in closing, I think this may -- I think this will probably transition to

some things that the panelists are going to talk about, that I think the demand-side approach is incredibly important and providing more information is essential. I don't think it can entirely solve the problem.

So, one, like, you know, not all security threats are felt by consumers, right? If my smart refrigerator is being used to DDoS Jared, I may not care, right? It's not affecting me, so I'm not really incentivized to price that into my smart TV or smart refrigerator choice.

Folks sometimes have trouble assessing security risks. One, this is complicated stuff. A lot of folks don't necessarily understand all the security ramifications from a connected or smart device. Even if they did, consumers are not necessarily great at assess tail risk, right? This is a essential part of behavioral economics. People underprice risk, which is why, you know, we made the policy choice to mandate seatbelt use in cars.

Testing will provide imperfect data. We don't have access to everything, so we're trying to input more information into the marketplace, but it's not as precise as -- you know, this company is providing $13 worth of security. It's necessarily a

lot more “lossy” than that.

And attribution is going to be -- is always going to be delayed and if at all possible in the security space. If my information -- if I'm subject to identity theft five years down the road, they may not know that it was X company's practices that did that five years ago. So there's definitely some kind of disconnect between my market choices there.

So for these reasons, I think it's kind of essential that information's important but we probably -- we definitely need policy enforcement as well, so encourage the FTC to encourage what it's been doing under Section 5 but ideally with a dedicated security statute, too.

And with that, I'll turn it back to you all.

MR. HO: Great. And thank you, Justin, for that presentation. And I know that we'll be returning to questions about the tools available for consumers to comparison shop based on security later on in our discussion.

But, first, I want to turn to a polling question. And it's really more of a scale than it is a polling question but so in our last panel, it was suggested that, you know, some folks were not entirely convinced that there is a consumer demand for security

or that perhaps that consumer demand isn't quite there yet. And I think that this spectrum or this polling question sort of gets to that.

And, so, you know, I'd like to sort of ask our panelists sort of what their thoughts are on the consumer demand of security and sort of where you think that we fit on this scale. You know, on one end, you know, is security important to -- is security important to consumers and who bears sort of the responsibility for security? Do they expect that firms bear the responsibility solely or do they understand or appreciate that it's a shared responsibility between firms and themselves?

You know, is it a moderate sort of appreciation or demand for security, or do folks feel as though consumers don't expect security in the products or some, you know, other category?

So why don't we start with Rick, and we can go down the line.

MR. WASH: Sure. I really like this question. There's a logical option that's actually missing. It says firms are responsible; there's a shared responsibility. The third logical option is that consumers are entirely responsible, and that's actually not an option in this, and I think that's a

good thing.

So my opinion, in my experience and in my work, I found I think B is the closest, that people seem to really think that security is important. People I talked to, they spend a lot of time trying to figure out, especially as they use consumer devices, as they use apps and websites, they try to figure out what they can do to help security.

They often see it as a balancing act between what it is they're trying to accomplish and what the security goals are. I hear a lot of end consumers talking to me about how they are told something that they're supposed to do about security, such as don't write down your passwords, and then they realize that they can't get their -- they can't accomplish their goals if they actually follow the security advice that they've been given, and they spend a lot of time trying to find a middle ground.

So it's not that they're just going to ignore the security advice; it's that they're going to try to find a similar advice that they could give themselves that they feel accomplishes the similar security goals but still allows them to get their work done. And, to me, that's a real sign that they think security is really important, but they see it as kind

of a shared responsibility. They don't know -- they know that they don't know everything about security. They look to advice from experts and advice from people like the FTC to try to figure out what they should be doing, but then they have to adjust that advice to whatever situation they're in and what their life is like.

And that adjustment process is the really hard part, and I think that's where things are getting lost a little bit right now. So I would say B. People mostly think it's important, but they see it as a shared responsibility between themselves and the firm.

MS. MARTIN: So I agree with you, especially around when we think about at the workplace. I wonder about consumer-facing products if it isn't closer to A and that they don't see themselves as being a point of vulnerability to a larger system. I think when we're at the workplace and we have to not write down our passwords and we have to have two-factor identification and all the academics get really mad and they don't want to do it, but we kind of understand that this is part of the larger system, that we have to do it to keep our system safe.

And I don't know that they see it as a shared responsibility when they set security on their refrigerator or they might see it on my phone and I don't want my phone to be hacked and made into a brick but not as a part of a larger system. Similar to when in -- not that they shouldn't. They should see it as part of a larger system, but I'm not sure that they do.

Interestingly, we do think of that that way around regular security with, like, the ideas of see something, say something, that we're all points of vulnerability in a larger system, but when it comes to cyber, that messaging doesn't come through. There isn't that constant vigilance. So I would put us at A.

MR. HODGES: I think I would want to get a hybrid of some of these, of course. I want to pick and choose because I think that the concern about security is uneven. I think that consumers tend to place a high value on security in situations where they understand that there are security implications of the decision they're making. So one of the most salient examples being exchanging payment credentials of some sort because they've been conditioned to expect that that's a security moment in their lives.

But I actually believe that they don't understand always the implications of other things that are at least equally important to security. For example, I think updating software is a very important part of security, and it's something that I think the vast majority of consumers don't necessarily have a firm grasp of in terms of its implications.

And, so, I think that they sense importance to it in certain situations, and in others, they have absolutely no idea. It might be the externalities that were referred to earlier, of, you know, why does Bob care if his smart TV, you know, is DDoS-ing Mary's network. And at the same time, I think that there are situations also where that risk to themselves and other situations becomes more visible. So in the news, there may be something.

So at a moment in time, I think a consumer may have a great awareness of security and a great demand for it, but I think on average, on any given day, it's kind of an uneven thing.

MR. HIGGINS: I guess I'll be a little bit of a naysayer here. I think there's an F here. Present company excluded, I don't think the consumers really think it's important at all. And I say that with a lot of background information with what the

consumers are doing. I think they are more concerned about that large-screen TV being able to be 4K or play Amazon than they are about the security that's imbedded in the TV to prevent Amazon seeing what they're watching.

I don't think Best Buy, if you go to a Best Buy tech employee he'll ever -- he's answered any security question probably in the last month about the security of a particular 4K TV. I just don't think, I think -- and it's based upon what Justin said, the externalities. We've made security violations of consumers to be painless. We have made the fines for stealing a credit card $50, and nobody ever charges that to the consumer for losing his credit card because they're afraid they'll cancel their credit card and go to a different credit card carrier. So they move around.

We've made -- banking fraud was so pervasive a few years ago before the nine federal agencies got together and mandated every bank had to institute two-factor because each bank was afraid because if they instituted and put security in the consumers would rebel and go to another bank. So I think we wish that consumers were more important and more concerned about security, but I think their actual feet on the street,

what their behavior is telling us is, sure, if you ask someone as they walk by, do you think security's important on your smart thermostat you have at home, of course they're going to answer yes. But do you think they asked the question when they were buying it about what it's doing, where it's reporting, who is seeing the data out of it? I just don't think actions are speaking much louder than words in my opinion.

MR. BROOKMAN: Yeah, I think that's fair. I mean, I was inclined to kind of come down in between on moderately important because I think people generally, as to privacy, they have a vague sense of there are things out there that could attack them, but I think when they're buying a smart TV, they're not thinking of it because they're not aware of what any possible risks could be, right?

I mean, when we did our story on smart TV privacy, people were very surprised, like, oh, it never occurred to me my TV might be listening to what I would do. It never occurred to me that if I type in my credit card information on my TV, that if it's not encrypted, that it could be attacked.

So I think generally in the connected world people have a vague sense, like, yeah, this stuff's important. Being able to make individual choices,

which is why we're trying to provide some more accountability for it is actually quite difficult.

On the whose responsibility, I think that this -- this I feel more firmly that I think people expect it to be taken care of for them just because, you know, the firms are the ones who are the experts here, right? If I plug in my new smart hub home at home, like I don't know, what should I be doing. Nothing occurs to me as a consumer about what should be done.

I expect that that's part of the product that I bought, that the experts will have put in place systems for authentication, systems to address all the things that we looked at. I mean, a consumer is not going to know whether there's a bug bounty program, right? So I think it's part of the default expectations that this is a responsibility of the company.

MS. MARTIN: Can I just add -- I was just going to say, I think there's two different things going on here. One is, is it important to them; and the other is do they trade on it in the market. And those are two completely different questions to ask. So is it important to me that my oven doesn't combust and catch on fire? Absolutely. Do I ask if it's

going to combust and catch on fire? No. I just assume it's not going to do that.

And, so I think that there is just an assumption, and I'm not saying that this is correct, there needs to be greater understanding by the consumers, but that's why they're so surprised when we ask them, did you know that Amazon is getting access to this data? Did you know that the data aggregators are sniffing up all of your information? Those are privacy violations. Do you know that this was a security violation? And they're like, no, I would never have been okay with that.

So I do -- I think that they think it's important, but they just assume like other certain product features that the firm is taking care of it. And, so, they aren't trading on it in the marketplace. So that would explain their behavior, and yet they're still shocked and upset when they find out there's been a security violation.

MR. HO: So, Kirsten, that's actually sort of a great segue into sort of our next conversation slide on the tradeoffs. What are the other factors that consumers are -- that might be considering and that might go into the demand question.

But before we get there, so it looks like we

have, you know, a panel of highly esteemed guests, and we have one A -- it looks like we have one A, one B. Justin, I think you're more on the C line, and then we have an E. So, you know, we can sort of see that there's a wide range of sort of thought on this issue, and so I think this next slide might sort of get us into the conversation as to you know, why is there this discrepancy, are there other factors at play.

You know, there certainly are. You know, you flip on -- you know, you turn on the paper, you read an article, and there's a security incident almost every single day. What is the reason for consumers buying, you know, poor security products? Does it have to do with any of these factors on the list?

And with that, I'll turn it over to Mark.

MR. LUPPINO: So, I mean, another prism that you can think about this is kind of the prism of product design, right, on the firm side. So how do firms balance these competing concerns of consumers that are kind of listed on the slide with concerns about security? And the way they do that, is that consistent with consumers' true preferences. And is it useful to think about this problem in these terms of tradeoffs? We can start with Justin.

MR. BROOKMAN: Well, I don't design products for a living so I was going to someone who does.

MR. HODGES: Okay. I'll hop in since I do design products for a living. I think, you know, one of these strikes me as kind of a strange outlier, and I know it's weird, it’s top of the list, cost, because I don’t know that -- I think Justin even mentioned it earlier. Like a consumer doesn't really understand the $13 worth of security. And, frankly, that unevenness I mentioned also is reflected in what our customers demand. So we have some who actually demand a great deal of security from us, others who demand none at all, and we need to meet everyone somewhere that we can all be comfortable with.

All these other things are tradeoffs against one another, though, and in general, our experience is that we see the highest utilization and most satisfaction with security features that are automatic or nearly automatic, and our experience is that we improve security outcomes and we nudge or make invisible things that are good security practice.

So great examples are, you know, we found a few years ago that less than half of our users were setting passcodes on their phones, and that was a not good thing because that's a foundational element of

security. And when we did a little -- honestly, not much, it didn't take long to figure out what was going on -- a little research, we found out they were unlocking their phones on average 80 times a day, and that kind of presented to us exactly why they weren't setting passwords on their phone, the friction.

And, so, that's directly what led us into looking at biometric authentication, our touch ID feature, and later face ID really reflect that desire to make something that's a much more natural and fluid way of interacting with the device and still preserving, you know, some amount of security, hopefully a very good amount.

We also see this with things like two-factor authentication. We rolled out various forms of two-factor authentication for Apple ID, for example, many years ago, and the adoption was abysmal. And part of that was on us because we didn't really work to make it seamless and transparent. Now, if you're migrating from device to device, people don't actually realize this, but very often they're actually effectively setting up a two-factor authentication system and installing tokens on their devices and all kinds of things, and it's happening completely behind their backs.

In some ways, I don't love not being transparent about security, but as a marketing person, I would love to trump it, what it's doing for you, but also the fact that sometimes we don’t love the idea of not being fully transparent with our customers what's happening, but at the same time, we’ve found that that's where we get often the very best outcomes from a security perspective.

So I’d say usability is probably the king here, productivity along with it, and functionality very nearly. I think latency is an odd one. I think it may apply more to things like e-commerce situations and things like that. From our perspective, what we see is that various technical innovations are continually removing any sort of computational or time cost of the security feature. So we're not really seeing that being nearly as big a factor.

MR. HO: And, Wiley, just to follow up. So this slide is framed as tradeoffs, suggesting, you know, one or another approach, but some people have suggested perhaps it's more of like a scale or a spectrum. And, so, you know, whereas the cost might be a factor, there might be sort of a solution, so you don't need to give up security for, you know, any one of these things. And, so, how does sort of Apple

approach that on any of these factors?

MR. HODGES: Well, I think the answer varies with the specific aspect of security. And, so, I think a lot of it is an approach. You could call it an iterative approach basically, where we will try something that we think is encouraging a good security behavior, we'll measure its effectiveness by looking at uptake and the way our customers employ it, and we will look at how we can improve that outcome as we go forward.

Usually, what we see is that users are prioritizing what I would call productivity or usability above almost everything else. It's the convenience that really governs their behavior, and so like I said, building things that are automatic or invisible really is what gives us the best outcomes.

There are some situations where we won't do that. A good example today still is software update, where we want there to be some affirmative user action associated with it, in part because we think it's a moment that a consumer should have some control over, but we also want to strongly encourage that moment to happen because we believe there’s immense security value in doing that.

So sometimes we're balancing that ourselves

to look at maybe it's a little more inconvenient this way, but we also want the consumer to have a sense of control, because that also goes to building trust with the consumer, which we think is an important part of having them, you know, have a sort of constructive security relationship with us. So when we ask them to do something, they might believe it's for a very good reason.

MR. WASH: So in addition to that, I really like the point you made about how there are some things that when we can, it's really great if we can just kind of automate security. In an ideal world, it would be awesome if we would just say, hey, we made this secure, you don't have to do anything, you don't even know about it, but in practice, there's a lot of things that where the users and the consumers have to be involved in the security aspects.

It's interesting that you brought up software updates. I've actually done a lot of work on software updates. And one of the things that -- there's an interesting, really clear tradeoff around security and then usability because software updates often change functionality.

And, so, if I -- and often the security ones do because they're preventing something happening that

shouldn't be happening, but then they change the way things work. And if you start changing things underneath people, they can get upset. And, so, there is actually an intentional choice that consumers end up needing to make about how to trade off security and software updates. And that comes up in a lot of different security situations where you can't just entirely remove the user from the security decision.

Authentication is another one that you came up with, which is, like, there's no way to remove the user entirely from authentication. That wouldn't be authentication anymore. And, so, we have to get the users involved and the consumers involved in these -- in a number of these situations, and that's where we're running into the real challenges.

You said it's somewhere between productivity and usability, and I agree. A lot of times, when I talk to consumers about how they think about security, the answer is -- they don't answer with the security answer. They tell me why they're trying to -- something they're trying to get done. So they look at their phone and they don't see a screen, they see this is how I talk to my mom at night. And that's the important thing, is they want to be able to accomplish these things in their life that have meaning for them,

and the security is the ability to do that.

And, so, they see security as an enabling feature when they can and try to figure out how to use it. And I've heard that over and over again.

MR. HIGGINS: I think over the years, over the last decade or so, we've done, and Apple has led the way on it in many instances, we've done a good job at making security the formal setup. You're secure when you set up a machine; you're secure when you set up a router, but routers for more than a couple decades came preloaded with a user name and password, and you had to actively go in and change it. You had to make a step and change that password and user ID to do it.

And if you had that selection and didn't do it, well, it still worked. In fact, you just plugged it in and it worked. It was a great router. Unfortunately, there was no security to it, and everybody that knew that user name and password could get into your router and do all sorts of bad things to your life. But it took us a decade or more -- more -- to convince the router manufacturers that, yes, that would impact usability for about a microsecond as people were setting up their routers, that they have to select a password, even if it was weak, we thought

a different password than the default was better than nothing. Not much better than nothing, but better than nothing.

So I think it comes down to productivity with the users. I can't agree more. You know, usability for the user is the principal. When we set up New York Times online, I was there when we were setting that up online, we set it up with a very low threshold for password when you first logged into your account. You're allowed to have multiple users in your account so that you could have your child logging in from college and using and reading the New York Times online. Or your husband could, on the way -- on his iPad on the way to work, as well as you sitting at home.

And we slowly -- we call it boiling the frog -- but we slowly started adding security functionality and reduced the threshold to the accounts being misused. There was no harm to the consumers because consumer protection was one of our caveats when we set it all up. But the protection to the IP, the intellectual property, the news every day was important and we started tightening that down over time to the point where it's ten times more robust today than it was when it was first rolled out.

And we did it over time because it was usability. If we had put that level of restrictions on those accounts, those first few days months and weeks of when we did it, users would have never adopted it. They would have gone to the next online newspaper and used their services because they didn't have that inherent level of security on. So it's important. It's a balance for a company to make.

Usability is always going to be king, but you've got to trade -- you've got to balance that with security and understand that people, in spite of themselves, still need to be protected, and especially in their procedures. So I applaud what Apple's done over the years. You have to now physically turn off your little PIN number on your phone. You have to make a positive action and say, no, I don't want security where it used to be; no, I want security.

And everybody, I guess, in this room would say I want that security and I want that privacy. But, you know, now it comes default and you have to actively say, no, I don't want it. And I think that's a big step forward for the industry.

MR. BROOKMAN: These balances are things that we're having trouble -- we're thinking about when we're trying to evaluate services, right? So if we're

giving someone a score for security, do we -- you know, is it most secure, or is it most reasonable secure under the circumstances, right? So if you have like a phone that doesn't connect to the internet, you know, that's pretty secure, right, but how do you take into account the other issues?

I mean, I know, like, we were looking at home security cameras the other day, and one service doesn't have cloud storage. It all goes locally. And as a privacy advocate, I'm like, that's awesome, like just have it stored locally, and they can never get their paws on it, but, then, again, that has, like usability. Like if you're, you know, somewhere else, like it may introduce other security elements as well, as we heard about security elements of home servers. So how to balance these things.

Like the example you come up with automatic updates, like I said, like automatic updates, like, are -- are -- get points, right. They are something that we look to, but the elements you articulated are also exactly right, like, there should be some consumer agency and control over that, and so there's maybe some degree of friction saying, yes, I understand the security update is appropriate, so maybe that should be actually -- maybe you should say

the push plus okay is the optimal result. And, so, trying to balance them into either overall scores or even just security-specific scores is tricky.

MR. HO: Okay. Rick, I'd like to sort of discuss a little bit more the consumer aspect of, you know, consumer expectations. And you've written a fair bit on this. And I'd also be interested in hearing what the other panelists have to say, but maybe you can start us off with sort of your research on the issue of information asymmetries. Is that something that exists in the security context and, you know, how do we resolve that asymmetry? Is it simply through more education, or is education not enough?

MR. WASH: That's a really good question. So there are two parts to that question. Do the information asymmetries exist and how do we resolve that? Well, one of them is easier than the other.

Yes, I definitely think the information asymmetries exist. There's a lot of information out there and it's really interesting, it's in different places. We did a project where we were looking at the kinds of information that was available to consumers about computer security, about cybersecurity issues. And one of the things we found, we looked at three different possible sources of information. One was

the kind of security advice that you see mostly coming out of the tech industry and places like the FTC or the FBI about how to protect yourself.

We looked at news organizations. And then we also looked at a collection of kind of stories that individual consumers have been telling to each other about cybersecurity issues. And what we found surprisingly was that there was very little overlap in the kinds of information that they were talking about. So a lot of the advice from the experts seemed to really focus on threats and countermeasures.

So what's the problem, and so, like, what is kind of technical aspect of the problem. So authentication, someone could log in as you, and then how do you deal with that. You have a strong password. Interestingly, those kinds of -- that kind of discussion almost never appeared in the news or amongst the security stories.

The stories that people were telling to each other focused a lot more on why -- who was doing this and why were they doing it. That's actually really interesting because currently, the way we're talking about cybersecurity doesn't really focus a lot on who the attackers and the perpetrators are and why are they doing this.

And, so, I went into that a little bit deeper to try to understand why is it that people and a lot of consumers seem so interested in kind of sharing speculations about, like, why would someone walk into my account as me. That was a really big issue that most of the discussions and the news stories didn't really talk about, and the answer was because they were trying to make these tradeoffs.

So as they kind of live their life, there are these tradeoffs come up, like do I have a stronger password and then have more trouble remembering it? Do I write it down? There's all kinds of tradeoffs to get made as they try to live their lives, and they're trying to understand these tradeoffs, and so to do that, they have to kind of envision the types of attacks and the types of problems that they possibly run into.

And, so, they really needed to know, right, if someone got into my account, who would that be and what would they do, because that really matters. If it's my kid sister getting into my account and making fun of me, that's a lot different than someone from another country getting in and stealing lots of money, right? Those are very different outcomes, and I would probably make different decisions based on that.

And, so, trying to understand why people or why these attackers were attacking things and what the process was and how do these security decisions actually then influence and prevent those attacks was really important. When I talked to people about two-factor authentication, for example, right now, I hear a lot of people know what it is, they know they're supposed to do it, but they don't understand how it helps. And that's the thing that I'm not seeing a lot in a lot of the consumer education materials right now is, all right, why is this a good thing? If someone was going to try to break into your account, like, why would two-factor authentication actually help stop them?

And once I start explaining it to them, where we've got a study we're doing right now where we're actually just sharing stories with people of ways that two-factor authentication stops an attack, and that seems to be very motivating, we're hoping -- that's what we're studying -- we're looking at an experiment right now to try to figure out to what extent that it is motivating, but that seems to be one of the key aspects is this information asymmetry and not what the security features are but why they work and who they help protect against and what kinds of --

and what things -- what things in my life they help protect me against.

So that also speaks a bit to the security education. I do think security education is very important. In my experience, the problem isn't related to motivation. Lots of people say they're concerned about security, and they seem like they really are, but they're trying to make these tradeoff decisions for themselves and their lives. And they feel like they don't have the correct information that they need to do that.

And that seems to be a lot of the problem that I'm running into, and that's why it may seem like people aren't making security decisions when they go and buy a television, but it's partially because they don't understand, okay, what does it mean. If Amazon has my TV viewing, what does that mean? What could they do with it, how would that harm me? They don't understand that. And usually there's actually good answers to that, but that's not part of what we're talking about when we teach people about security. And that is, I think, one of the challenges that we're trying to, that at least my work is trying to address.

MS. MARTIN: I think you pointed out there's like the scope-of-the-problem information asymmetry,

which is kind of -- which they're trying to talk about why would someone do this in general, what types of harms could befall me or everybody else with the cybersecurity incident, anything along those lines. And then there's like another level of when I buy this thing, what level of security am I getting, or when I make this update or don't make this update, like the very transactional information asymmetry, that happens a lot of times in the marketplace where they can't trade on something. They can't trade on it if they don't know about it.

And it's interesting because I think -- if we think about the flow of information in general, you have security incidents, which is an adversary, an outsider coming in, and taking information, but you also have privacy, which was mentioned before. That's the firm just telling stuff, right? That's a different thing altogether. That's not an outsider coming in. That's the company is saying I think other people should have access to your data, I might get a little money on the side, but this is how we're going to have -- I'm going to commit a privacy violation.

We have a ton of trouble giving that information on the privacy side of consumers so they can say I want to use an Apple device versus an

Android device, like we can't -- it's really difficult. The companies have a hard time putting that level of detail in a digestible form to say I want to compete on privacy. It's just a difficult thing to do right now.

We really have that problem on security, because I just think that the companies themselves don't always know where security vulnerabilities are. It's hard to conceptualize and explain to people. And that's actually where Consumer Reports does a ton of work because when you have a marketplace with the information asymmetries, branding and, like, putting a little sticker on that says Better Business Bureau, Consumer Reports, those types of things is a signal from a trusted source that's kind of a standard market solution to a major information asymmetry, not in the scope of the problem like you're talking about, which is more of cybersecurity professionals should just start making PSAs on, you know, like if you see something, say something, do you use two-factor authentication of take your password, you know, they should just make those types of things.

But this idea of if I can't figure it out myself, I look for a trusted partner to put a stamp of approval and say the equivalent of Intel Inside, or

this has been -- this meets a minimum security threshold, and that take the burden off the consumer. And I'm not sure that the consumer can ever be expected to understand what factors are important, because think about what they would need to know. What factors are important, which Consumers Reports had a bunch of professionals trying to figure that out, and they had to just come up with ideas. What criterium is success, and does this product meet that criteria. That's a lot. You know what I mean?

And, so, I almost think it's inherent to the problem that we're going to have information asymmetries and we need to not put the responsibility on consumers to buy the right product but look to companies to say, look, this is the minimum standard of security, this is best practices, this is just what we do. Or another one is Consumer Reports comes in, or someone like that, and says, this is the minimum standard, how do they do on that criteria. And that's the work that they do, I would say.

MR. HODGES: Yeah, so we're obviously trying to provide more information to the marketplace about the range of behaviors. But I do think -- I mean, it is also a role for policy here to say what the actual minimum is, right?

MS. MARTIN: Right.

MR. HODGES: I mean, this is something that you talked about earlier, that consumers buy something, they kind of just expect it to work. It's like the analogy of, like, you don't expect your fridge to explode, right? By that same token, there are some reasonable expectations when you buy something that there's some implied warranty that is going to work, it's going to have some degree of support going forward.

And, so, I know the Federal Trade Commission has done a little bit of work on this area, like, they've done warning letters against -- I know Revolve was a smart hub that was bought by Nest, and Google bought them, and it was kind of connected to everything in your house, and it relied on server support to work. And then one day, I guess Google was like, we have too many smart hubs, let's just shut this one down. But someone had, like, paid 300 bucks for it 18 months before and it just, like, turned off, right?

And in that case, the Federal Trade Commission said, well, no, they sent them a warning letter, saying, okay, because you're giving everyone their money back, we're closing this case, I think the

implication being, like, at some level that does become deceptive or unfair. And, again, as we're in the space right now where there are absolutely zero norms around support length, right?

I mean, at some point I think the FTC may need to step in and say, okay, if this particular device is vulnerable to lots of attacks, consumers are being attacked, we see so many IOT products out there that have just dire support practices, the FTC at some point is going to have to step in and use their Section 5 authority to say -- to at least put some barriers in the road about what's forbidden.

MR. HIGGINS: Well, most of this, most of the businesses, I think almost all the businesses now, have a set of standards from a security perspective that they abide by, even within the products that they're developing. And there's -- I mean, in fact, some of the jokes about standards, they're so great because there are so many to choose from, but, you know, that's the challenge of a business trying to set up its practice.

Usability, as I said, is the bottom line, but oftentimes, that is at a tradeoff. They trade it off and they trade off security for it, especially as a fledgling company, because they want to grab market

share quickly, as fast as possible, and really I think those are danger zone people. An established company, I think overall, there's a growth aspect that happens at some point. They get enough users behind them, they have enough of a reputation, they have enough of a brand name, and they embed security.

If they haven't done it before, that's when they get serious about it, but it is a tradeoff in the early days. Do you hire a new programmer to build more usability functions, or do you hire a security guy? You know, they trade that off every single time as a young company. Most big companies, because they do have these standards they have to abide by, are following the rules -- for the large point, are following the rules and are doing the right thing in building security into their overall processes.

That's not to say privacy because I think, I don't know about you, but, you know, one of the great topics around the turkey table this year was how many people had ever read a complete privacy document, privacy statement on any service or product from beginning to end on any product or any service they've ever bought. And the answer was nobody at the table had ever done it. In fact, most don't even get through the first page because it's just convoluted

lawyer-speak. It's more litigation prevention than it has anything to do with a declaration of their privacy.

And, so, most people don't know what's in those documents and they don't know what the data that they're giving the company is for. It's very secure. They're sending it back to the host company very securely, and they're protecting it, but then what happens to it, nobody has any idea.

So I think the overall perspective and the overall industry is run on a risk level, and more importantly than anything else, companies are trying to protect their brand and trying to protect their reputation to be able to stay in business.

MR. LUPPINO: Thank you. We have a question from the audience. Currently, demand-side incentives for firms regarding security seem to be mostly back-loaded. Consumers leave due to a breach instead of being front-loaded. Consumers purchase based on security.

Is it important to push front-loaded incentives or are back-loaded incentives sufficient and how to be -- and how would it be best to push front-loaded incentives for consumers?

MR. HIGGINS: I'll take a shot first, I

guess. From a front-loaded standpoint having been in Corporate America for quite a while now, I'm telling the salespeople to sell security as a feature doesn't go over really well. They want to talk about the usability, the functionality, the interoperability, the resiliency. They want to talk about every feature. Security is in there. If you ever looked at a website for a product, if security is mentioned on that product at all, it's way at the bottom of the list. So it is back-end-loaded.

I think selling a product up front from a security perspective is an uphill battle today, and it goes to some of the security training that we don't do to normal consumers and infusing a security awareness in the general population that they should be asking those questions. So I think it is back-loaded, and that's the way it's going to be until we can change business practices.

MS. MARTIN: Well, one question is which market actor, I know the name of it is consumer demand, but I'll just say, I could see three -- I used to say two, but now I'll say three different market actors that could exchange money for security, right? Consumers, which I think we've all identified issues with expecting security to be something that's traded

in the marketplace of consumers. The other place that we look at businesses that have to get money is from stockholders, so public companies or investors and they can demand. And that's why probably it's being -- you know, there are some policies around it through the SEC, is because if you're a publicly traded company, there are certain obligations of disclosure that you have to explain so that stockholders can understand the risk you're taking around cybersecurity.

And the other one -- and that's -- so that's front-loaded in some ways. Like, you're saying I need to prove to you to get your investment as to what, so you can invest in me if I meet some sort of minimum threshold that you've identified, and especially for institutional investors, they could look at that.

And, then, finally, insurance companies. I mean, those are other market actors that you have to then front-load that decision to prove to them and they will trade on securities. So I know we're talking about consumers, but consumers are just -- and you could have -- there could be all sorts of market actors that actually are more likely to only do business with you if you meet a certain security threshold than consumers.

So if you're a target supplier now, I bet you they're going to be much more, you know, focused on the cybersecurity of their suppliers than they were prior, you know what I mean? Like, so I would just say there's more than consumers for market actors.

MR. BROOKMAN: Absolutely. Yeah. I would say, I mean, a couple things. So, one, some more requirements around transparency, right. A couple states have laws saying that you have to have a privacy policy, but they don't actually have to say what's in them. So privacy policies tend to be, like, super vague, like, yeah, we collect data and do stuff.

But if there is, like, a -- but if there's a requirement, say, that you have to do -- you know, you say X, Y, and Z in the policy, that allows maybe not consumers sitting around the table, but allows folks like us, allows folks at the FTC, it allows the press to introduce some degree of accountability in there for practices.

I mean, I do think it could be a good thing to push more companies to make affirmative promises of support going forward. You know, we're starting to see more of that around mobile phones, right? You've seen a number of Android devices promise to support periods for two or three years. And we have some more

expectations that, you know, desktop systems are going to be supported for a longer period of time. We don't have norms in IOT, I think. You know, some policy initiative to get folks to say that out loud in advance I think would help move the market in a good way.

You know, companies committing to data minimization up front, I think the example with ApplePay is a real good one, you know, Apple going out of its way to say, hey, we're not getting this. And this actually is one of the more prominent selling features of ApplePay. I mean, you don't often see a white paper link to the main page on security protocols on the product description page, which I think is a really positive thing.

And, then, like, I think there used to be just more questioning in advance, like do we really need to connect this to the internet? Like, a friend of mine, like, bought a washing machine and, you know, she spent, like, an hour getting it to talk to the router. And, like, I can imagine some peripheral use cases, yeah, if you want to, like, start the cycle on the way home so it’s not going to get moldy, and so you don’t have to start it in the morning, so, yeah, there’s some mold minimization, like smell issues.

But, like, by and large, like, I personally would pay more money for a washing machine not connected to the internet. And, so I think there's been this big, like, panglossian, and let's connect it all in Silicon Valley and other manufacturers. I hope we're starting to rethink a little bit.

MR. WASH: So my work is mostly on the use side more than the sales. So I think the premise of the question is that security matters more during use than at the sales point, than the initial point. And I think that's right, but my work is mostly on use, so that could just be because I study use.

But one thing that I've noticed, especially on the use side, is that there are different -- that security matters differently for different types of products and different types of information. The contrast that I like to draw is when I talk to people about financial losses, such as stealing your credit card, people seem to believe that, like, this is something that if someone steals my money, I can get it back. The banks are doing a pretty good job of giving me my money back.

However, something very different to compare that against would be photos of my kids. If someone steals and deletes the photos of my kids, there is no

way that anyone can give that back to me. And, so, the people that I've talked to seem to treat those situations very differently. And, so, you may look at something and see security, but it depends on how the consumers are thinking about what is it protecting, and that actually might lead to slightly different answers in different segments.

MR. HIGGINS: But that goes back to the question you asked earlier, why? Why is someone going to try to steal pictures of my kids, so they're much more freer to put that data out on the cloud in their instance because they think, well, nobody's going to go after it because why would they go after it.

MR. WASH: Yes.

MR. HIGGINS: So, you know, again, it goes back to harm and risk issues, their own assessment, it's a risk.

MR. HODGES: I would add, I think there's this other interesting challenge, you know? I totally agree with what Rick said and with what Mike just said, that, you know, these stories are a big part of how consumers inform their behavior. In essence, they're kind of doing threat modeling, but back to information asymmetries without a lot of information, and --

MR. HIGGINS: Structure.

MR. HODGES: -- right, yeah, and structure and formal methodology, all these things. But, ultimately, I think one of the challenges is always what can I do about it, because I think when you look at how do I prevent the loss of my photos, it's not immediately evident to every consumer every time what the right answer might be. And, so, I think one of the challenges is understanding, what are the actions or steps I could take, even if I fully understand the threats and concerns. I think in that sense, front-loading this a bit would be super helpful in helping consumers understand that there was at least a purchase decision they could make.

To Justin's point, I would also pay more for a new appliance that was not internet-connected. I don't know if you've heard the Betteridge's law of headlines, anything that ends with a question, the answer is no. I think that should be true of IOT generally. But that said, you know, we don't have a choice necessarily. And, so, I think one of the interesting challenges is giving customers a constructive choice they can make in a sense that they can actually take an action.

MR. HO: Maybe we can follow up on that,

given Rick's comment about how consumers treat different types of information differently. And, so, if there is a market or, you know, different tools, security features available to consumers, you know, what tools should apply in which instances? You know, take multifactor authentication, for example, as a consumer feature. Should it be applied across the board or in what instances do you protect information versus balance friction?

Anybody here? Mike or Wiley, do you want to start?

MR. HODGES: I might jump in. I would say one of the big challenges is always going to be making it work. It goes back to the usability tradeoff, right, and actually what Justin said about, you know, you can have the phone that doesn't connect to anything, it's not much of a phone. So we're always finding ways to trade off. And, so, for instance, with two-factor authentication, you know, one of the fundamental questions is is it always going to work?

I mean, there are actually situations where I would argue you should never use two-factor authentication because a loss of the second factor might lead to the complete loss of the data underlying it, like your photos, for example. So those kind of

things need to be built into the way you consider, and requiring it everywhere would be a pretty ill-advised policy in that sense.

I think customers are also going to be challenged with things like interoperability. You know, we can introduce the greatest security feature ever. If the entire industry doesn't use it or some critical number of players don't use it, it really doesn't matter. And, so, I think one of the interesting challenges remains how to provide widespread access to some of these kind of things, particularly around authentication, which remains one of the thornier problems, I think, to solve in a way that helps consumers without putting too much friction in the process.

MR. HIGGINS: Yeah, I'd have to agree. I won't even comment. I'll just let Wiley's statement go.

MR. WASH: I would agree, also. To repeat something I said, I'm not a product designer, but I study how people use a lot of these different products, and I think there's a role for giving people choices and for designing different products differently. So I completely agree with you.

There is also a role for providing

appropriate information and for providing kind of nudges or defaults that are appropriate. So I really like the examples that Mike and Wiley were talking earlier about how -- like defaulting to locking your phone and having to make -- take explicit actions to make it so that you don't have a PIN number on your phone. That seems like it makes sense. It still gives people the flexibility, but it kind of defaults to being secure.

And, so, I think having those kinds of expected best practices seem valuable, though while still providing some control to end-users to make those tradeoffs in security decisions.

MR. BROOKMAN: Yeah, I mean, I'm generally skeptical about efforts to make privacy protections contingent upon sensitivity, but I think in the security space it definitely makes sense. I don't want to have to get a six-digit PIN to open my refrigerator. I think that would be, like, suboptimal, and I would not want to rate that highly.

MR. WASH: So I also have -- I was just thinking about another study that I did that -- about -- it was about software updates, but it actually said something interesting about defaults, also. One of the things that’s been interesting about looking at

software updates over time is that we've automated the software updates more and more so that if you go back 20 years, you pretty much had to click manually to go even look to find out if you had them and then do another click or two to install them. Now it's much more automated. And it's been a slow process over the years of getting more and more automated.

And as we looked at this over the years, one of the things that we were noticing was we can't automate all updates. There's always a few that are kind of important enough that it's not -- we can't automate that. And people who had more experience doing software updates were better able to make those security decisions, and that as we automated it more and removed it from the user, it seemed like almost that they had been learning less about software updates and were actually having more trouble.

MS. MARTIN: Atrophy almost.

MR. WASH: Yeah.

MS. MARTIN: Your ability atrophied.

MR. WASH: The way I like to think about it is if you have a range of problems from easy to hard, if you remove all the easy ones, the only ones left are the really hard ones, but you don't have the ability to learn from the easy ones. And that was

actually an interesting -- so there's a consumer education, so product design is related to consumer education in really interesting ways.

MR. BROOKMAN: Yeah, I'd like to echo the point I made earlier about -- with the security updates and the potential for being combined with updates that potentially impinge upon functionality, right? So EFFQs, Epson putting in functionality to a security update, that would make it harder to use third-party ink cartridges, right, and so that has -- and there's like similar practices.

You know, Facebook accused of using phone numbers provided for two-factor authentication for text spam or for targeting ads, right? And, so, how do you -- how does the FTC discourage companies from lending -- from misusing information or permissions provided for security updates? I mean, I think, again, at some point, this may exist, may violate existing law, but otherwise, there may be some guidance the FTC can give to identify those sorts of things as bad practices.

MS. MARTIN: So that is interesting because you could imagine a company that misuses the security updates and then uses it for a privacy violation, which is what you just described, as really

undermining what we would call the institutional trust in security or online or information security in general, you know? And that would be -- and because a lot of times, security violations and privacy violations both hit my trust in a firm, but it also makes me distrust everything.

And, so, you can -- we do studies that show institutional trust will go down significant percentage points after hearing stories about privacy violations or, separately, stories about security violations. And, so, you can -- and public policy actually comes into play to preserve institutional trust on a fairly regular basis. I mean, that's one of the places where we don't let it up to firms -- we don't let firms decide if you're going to allow insider trading or not.

We take that off the table, and we say, no, no, no. We're telling you you can't because that undermines the institutional trust in banking. And, so, you can imagine the penalties for abusing a security update to be worse than just, you know, the standard privacy violation that you would have because of that institutional trust.

MR. BROOKMAN: Fully agree.

MS. MARTIN: That's interesting.

MR. LUPPINO: Thank you. Changing gears slightly, what types of security requirements have seen the greatest buy-in from consumers, which have seen the greatest amount of pushback, and why is this?

MR. HODGES: I mean, from my own experience, I would say the use of biometric authentication represents the greatest single success we've had in security and has the greatest buy-in by far. I talked about less than half of users setting passcodes. By the way, to use these features, you have to set a passcode, like that's sort of the carrot and the stick we have, is it will be easy, but you got to give us a passcode first.

And we went to basically, I think, recently, you know, high 90s compliance with setting passcodes. So it was a pretty profound shift. And that's one of the greatest successes, but it comes back to also being associated with convenience, right? We can essentially put in place a security technology that removes friction, you know, improves convenience, that's great.

And the other for us actually has been multifactor authentication for our Apple ID accounts. You know, we had tried doing this a fairly conventional way and found it didn't work very well.

We've instead tried to make it as seamless as possible, and, once again, we found that by doing little nudges into it, like encouraging users to do it during the setup process, for example, we're getting much, much higher compliance. And the key is the cost has to be low for the compliance to be high. I think that's really the net we see in every case.

MR. HIGGINS: And I would add probably the one that doesn't get noticed a lot is the sleep function on the phone. It saves battery, it keeps your phone on forever, you know, you can get to a charge station before you need to charge your phone again, but what it provides you is physical security. You have to have your password. You have to have your thumb print in order to open the phone again. And, so, a lot of the old attacks of leaving the phone at the bar and someone picking it up and walking away with it and just being able to get into it have gone away because the phone is in sleep mode and can't be broken into.

So there's a lot of inherent security that goes back to the concept that security needs to be as transparent as -- not as transparent as translucent as possible. It needs to be -- users just can't see it. If they don't see the security happening but you're

providing them security, and a lot of big corporations do a very good job of providing that security for their product or service, if you're doing that, then the security is being used by a lot of users.

If you're not doing that and you're making it intrusive into their daily operations, something as simple as, you know, yes, you have to multifactor into things that you've never multifactored into before, you have to enter a PIN for doing certain things, it becomes intrusive and people will find a way or find another service that they don't need to use that service. So it's all about usability and functionality at the end of the day for the consumer, I believe.

MR. WASH: So I like your example of the biometrics. Before that, I would say passwords were a really successful security technology. I don't know anyone who doesn't have at least one password, so that is a security and a technology that pretty much everyone uses.

MR. HIGGINS: I've got a four-year-old granddaughter. I don't think she's got one yet.

MR. WASH: She might, actually.

MS. MARTIN: Yeah, That's true.

MR. WASH: But another thing to think about

the translucency that's really interesting is one of the challenges that a lot of the security instances that I come up with is, is there seems to be a really big difference between taking positive actions and recognizing things that are present versus trying to notice when security's not there.

So one of the really big challenges that a lot of security has had is when -- if security is there and there's some kind of indicator that says, look, there's security here, but then sometimes that goes away. It's really, really difficult to notice when something's missing, and it requires a lot more expertise in understanding what's going on and why that might or might not be missing than it is to notice that something is present.

And, so, that is a -- it's a really big difference, and a lot of the -- as we make security defaults, we're seeing this more where there is defaults to security but then sometimes -- like if someone turned off the PIN number on your phone and you didn't know it, how long would it take you to realize that? That's a hard question, and actually I don't know the answer to that question.

But that kind -- so there's different types of security about present versus absence that actually

seems to make a big difference for people's ability to recognize and make decisions based on that.

MR. HIGGINS: A good example of that would be the lock, the SSL lock.

MR. WASH: The SSL lock, yes.

MR. HIGGINS: When it's not there and you're -- how many people go to websites now and you just expect that any kind of PCI transaction is in a secure session, and when it isn't, how many people really notice it isn't?

MR. WASH: Yeah, there's been some research that says very few.

MR. HIGGINS: And our DLQ tools and the companies find it when it isn't.

MR. WASH: Right.

MR. BROOKMAN: The friendly part is going to make browsers make choices to really highlight that and to kind of really push people aggressively to using SSL. On the biometric side, I would point out that I think they have been fairly effective, and I'm a big fan of them when deployed correctly, but obviously, like biometrics are incredibly sensitive, and I think the -- I think Apple and some of the other leading manufacturers have been very careful to make sure the data is stored locally, on the device,

potentially in a secure element.

But I think you could run into problems if, like, a biometric database gets leaked and then I think you run into this problem -- some of the problems Kristen talked about, how you ruin it for everybody. But kind of -- and more directly there if people can access the raw files of people's fingerprints, so while I think biometrics can be very useful, I also want to caveat that with some concerns about, yes, as long as it's done right.

As far as ones that I think people have pushed back on, I might as well give a shout out to companies that make you change your password every two months. That's something that I know a lot of folks have found to be frustrating. I know when she was chief technologist here, Lori Cranor wrote a good blog post about why this is actually bad security practice, and in addition to I think recent compliance costs can actually create more of a corpus of information if hacked that could actually make it easier to guess passwords.

So that's something I know that a lot of consumers that we talk to like rebel against and I think is probably, hopefully, is getting to the point where it's no longer recognized as an optimal security

practice.

MR. LUPPINO: So, actually, following up on that, what is the scope of third-party services such as password managers some of the security burdens on consumers?

MR. HODGES: I mean, my own perspective is that there's a lot that they can do potentially. I mean, you know, obviously, we have our own password-management features that we deliver, but also have some really great password management apps that run on our platform, and, in fact, we just recently did some work in our latest OS releases to help them integrate better with the system, but I'm sorry to say I don't think that market has proven very large.

I think, you know, going back to sort of what's consumer demand for security looking like, well, look at the market for VPN services, password managers, and products along those lines and, you know, it's there, there's clearly some interest, but it's not immense, and it's nowhere near the size of the market for 4K TVs, for example.

MR. BROOKMAN: There's not immense, but I think they're both growing, right?

MR. HODGES: Yeah.

MR. BROOKMAN: I think there's probably

adaption to both, and like -- and then you look at something like ad blockers, which are another third-party tool, and the use of ad blockers is, like, getting a lot -- has close to, like, 30 percent. And, again, that's free, right, and so that's maybe one element as part of it, but I think there is growing market for privacy in general that does include third-party tools. Again, it's not all the solution, but I think the trend lines are positive.

MR. WASH: One challenge with that is integration. So a lot of tools are difficult to integrate with. Apple's a great example in that they just recently in one of the more recent versions of their operating system allowed the third-party ad blockers to use some of the operating system features, and before that, they were a lot harder to use.

There's still a lot of services out there that don't allow third-party integration and that I think limits the abilities of third-party tools to solve that. And, so, that in some ways the lack of integration limits the market.

MR. HIGGINS: I think you're right there. When you're dealing with consumer products from that perspective, your product that you just developed, your third-party product that you just developed has

to work with an infinitesimal number of configurations and systems out there, from PCs to mobile devices to, you know, to network and devices. It's just -- it's all over -- and you have to keep them -- hopefully you maintain support for all of them.

So you can't just sell a product out and say, okay, it's only going to work for this version of this because your market's going to be that much reduced when you realize that there are people out there that are on -- let's see, I think I heard the record was something around 32 versions old on an Android device. You know, it's, like, crazy. And how can you build a consumer product that is sufficient from a security perspective on something that old?

MR. HODGES: I will add to that, just to put another little tone of maybe -- I'll call it news, not bad news or good news. As a platform vendor, there's this interesting balance and tradeoff we have to make, which is to provide entry points for people who build these kinds of third-party products like ad blockers and like password managers while simultaneously not creating so much new surface area that we are presenting great opportunity for attackers, which we're always concerned with. And, so, that's a tricky balance and definitely one that we struggle with on an

ongoing basis.

MR. HO: Okay, I'd like to use the balance of our time to shift gears and talk about tools that consumers have available to comparison shop and shop based on security. So Justin talked about this a little during the beginning with his presentation, but I'm curious to hear what other folks think. You know, is there a market for consumers to shop based on security?

MR. HIGGINS: I think consumers comparison shop everything. You know, they do comparison shopping, they're -- all the time. Some of them, my relatives, use CNET, use Consumer Reports all the time. I mean, I think there is a market for the ability to not only look at standard functions, usability features to it, but it's more important now as consumers are becoming better educated, and there is a small subset that are, as they become more educated on what privacy protections that particular product has.

Again, in house, I was looking at Thanksgiving, and one of the questions I asked was how many people in the family were using some sort of Alexa-like product in their home, that had bought the device to ease their use of some of the IOT devices

they'd gone out and purchased. And the ones that were not using it were concerned for privacy issues. They had read the news articles about how it's always listening and they can't trust it yet and all sorts of issues around security and privacy.

Maybe that was my influence, hopefully, but, you know, the ones that weren't looking at a function -- or were using them were using them from a function of they did their research and they did -- and they felt comfortable and they trusted the brands that they were buying. So I think overall there is a good market for those types of research, and the more the better.

MR. BROOKMAN: I'll reiterate the point I made earlier about, you know, I think there's more that can be done. I think given that there's not a lot of affirmative requirements to make information available, to make products testable, and actually in some ways it's getting more difficult to test products in some ways.

I know this is a conversation we had at one of the PrivacyCons that the FTC hosted a couple of years ago, that sometimes it’s actually getting more difficult for researchers to peek under the veil to see what's happening, and then, like, beyond that,

we're seeing some companies actually kind of going out of their way to affirmatively, like, actively frustrate testing. And, so, again, this is an area that potentially the FTC could bring some more actions on.

You know, like, I think the Volkswagen case was an example when the FTC did bring action, that trying to fool regulators in terms of testing emissions in the lab, trying to look for the specific testing conditions. But they may need to go farther than that because I think there the representation's based on, you know, statements to regulators that, hey, we're compliant with X, Y, Z. You know, we may need -- and this is a comment I made at the previous hearing on artificial intelligence, but, you know, we may need to expand the concept of deception to include, like, you know, tricking not just consumers but tricking testers, tricking user agents, tricking the Safari browser, tricking other things that aren't quite exactly consumers but are still as software and other things kind of intermediate more and more on the information we get and may need -- we need to expand, you know, what we consider to be adding misinformation to the marketplace than currently in the FTC tool set.

MR. HO: And, so, Justin just mentioned some

challenges, and, you know, he also certainly mentioned some during his presentation, you know, update frequencies, it might be sort of difficult to look under the hood. What do you guys think about those challenges? Are there others that you didn't mention?

MR. HIGGINS: Well, just on website use, I mean, there are commercial products available for companies to buy where you can see the number of and the types of places that your employees go to and rate those websites based upon the types of everything from its privacy rules to its contract use for how it should be used, the user agreement that you click on as you go onto the websites, to the security of the website itself. And those are available commercially, but they're largely not available for consumers.

It would be really great if some of those tools out there would be available for consumers so that just mere surfing could take on a brand new activity so that they could look at it and say that, yes, if you go to that site and you use that site for this following action, you know, they fully understand what they're doing when they go to that site and the privacy that they're giving up when they go to the site.

So almost to me, those commercial companies

that are doing it for commercial businesses should be doing it for consumers, but there just isn't a market yet for it. They can't figure out how to make a business plan that could sell this to consumers, but if they could, I think it would be a great step in the right direction.

MR. HODGES: I would actually add that I do think transparency remains a struggle in determining these things, and, you know, vendors may be opaque for good reasons, like they want to simplify a message and make it easy for someone to understand or for evil reasons. And it actually, like, reminded me of this when I was thinking about it. I actually have seen a consumer tool that's a plug-in for the web browser that actually does a similar thing. And about 80 percent of the websites it marks as insufficient information to judge.

MR. HO: Thank you.

MR. WASH: So if I have a second. One of the things that I've observed is people seem more willing to talk to each other, and there's a lot of word of mouth than I've seen in the past. And that seems to be increasing. So when I first started doing research with end users, I would hear worries about talking about security would make them seem like they

were a tinfoil hat type of person. Now, I have no problems finding lots and lots of people who have heard multiple stories from other people about security issues, and they find them interesting, and they share them with their friends and they talk a lot more.

And, so, I think there are cultural changes going on about willingness to talk about security with other people that are really important. I mean, Mike just talked about having a security discussion with his family over Thanksgiving dinner, which seems like a very normal thing to happen now, and 20 years ago, I'm not sure would have been seen as normal.

MS. MARTIN: I think one small thing that would just be an issue in the future is we've come up with lots of solutions about the architecture and how it can solve security and usability problems, how we can have nudges to help people along, make it seamless to the user around security, how we can actually give better notice, and there's this effort to kind of explain to people why security's important, whether or not we disclose it to the SEC or to our investors or our consumers or our suppliers, and they're really good about it.

I think the more work that’s done in that

area, the more it's hard to understand the answer around privacy, which is there's no way to explain this, it's too complicated. There's no solution that will ever be mutually beneficial. So that answer around the flow of information when there's an outsider versus when it's the actual firm selling the information or access to it, it sounds disingenuous. They've tackled a harder problem in some ways.

And, so, you could see the arguments of looking at those things and saying if you solve this, now go solve that, you know, go solve privacy. Or if it's hitting institutional trust in the similar way if we're regulating security minimums, you could see them turning around and saying, okay, now do privacy. So I think even though they are very different, they're different actors, they're related in a way that you could see them regulated in a similar way.

MR. HODGES: No, I mean, I totally agree with you, Kristen. The one thing I would note is sometimes they are actually very much in opposition. And, so, a great example is that, you know, laudable as PCI and its related requirements are, it actually requires Apple as a company to collect information on customer transactions that we'd actually rather not possess or not hold onto.

MS. MARTIN: Yeah.

MR. HODGES: And, so, I think there are cases where we see that well-intentioned security policies actually can be very much intentioned with the -- what I think are the best outcomes for privacy for end users.

MR. HO: Well, thank you for those last comments that do very well in tying security with our hearing in February on privacy. But with that, I'd like to thank our panelists for their thoughts in this conversation surrounding the consumer demand for security, and I'm delighted to turn the time over to Jim who will give closing remarks. Thank you.

MR. TRILLING: Good afternoon, everyone. I'm Jim Trilling, another attorney in the Division of Privacy and Identity Protection here at the FTC. I want to just briefly, on behalf of the Federal Trade Commission, thank all of our panelists for the excellent discussion today and also thank both our in-person audience and our online audience.

We look forward to continuing the discussion tomorrow. The panelists today have highlighted a number of issues that we'll be discussing more in-depth tomorrow. We'll be beginning at 9:30 back here at the Constitution Center with a panel on data

security assessment. That will be followed by a fireside chat between FTC Commissioner Rebecca Kelly Slaughter and Joshua Corman, who among other things is a cofounder of the “I am the Cavalry” security initiative

That will be followed by a panel on the U.S. approach to data security, and we'll wrap up the day with a panel on FTC data security enforcement, and then closing remarks by Maneesha Mithal, who leads the FTC’s Division of Privacy and Identity Protection.

With that, thank you again for coming, and we'll see you tomorrow.

(Applause.)

(Hearing adjourned.)

CERTIFICATE OF REPORTER

I, Linda Metcalf, do hereby certify that the foregoing proceedings were digitally recorded by me and reduced to typewriting under my supervision; that I am neither counsel for, related to, nor employed by any of the parties to the action in which these proceedings were transcribed; that I am not a relative or employee of any attorney or counsel employed by the parties hereto, not financially or otherwise interested in the outcome in the action.

s/Linda Metcalf
LINDA METCALF, CER
Court Reporter