U.S. Senator Maria Cantwell

U.S. Senate Committee on Commerce, Science, and Transportation Hearing Titled, "Enhancing Data Security."

Witnesses: James E. Lee, Chief Operating Officer, Identity Theft Resource Center; Jessica Rich, Of Counsel, Kelley Drye, Former Director, Bureau of Consumer Protection, Federal Trade Commission; Edward W. Felten, Robert E. Kahn Professor of Computer Science and Public Affairs, Princeton University, Former Chief Technologist, Federal Trade Commission; Kate Tummarello, Executive Director, Engine

October 6, 2021

Opening Remarks

[AUDIO] [VIDEO]

Cantwell: The Committee on Commerce, Science and Transportation will come to order. Today, we're having a hearing on enhancing data security. And this is about the second in the series of hearings that we're having on the importance of good federal standards for both privacy and data security. Our first hearing focused on the empowerment of the FTC with new resources and the Data Privacy Bureau that is being considered as part of our reconciliation negotiations, as well as hearing from the witnesses what we should be doing to enhance further data privacy.

Today, we want to focus on data security, and the fact that we are seeing record levels of reaching and intrusions on the privacy of American individuals. In our hearing today, we'll hear from a great list of witnesses that I will mention and more formally introduce in a few minutes. The data systems that we write rely on today are very vulnerable. We are experiencing increased rates of data breaches and are now seeing sophisticated actors impacting hundreds of millions of American consumers. I think that we are going to hear from Mr. Lee's report that 2021 will again set a record year for the number of data breaches and concerns to consumers in the United States. What's troubling about that, is that every year we are breaking records. What's troubling is that these breaches are now more sophisticated, and that we don't have the adequate security to help stop them.

Earlier this year, a hacker took Colonial Pipeline offline, causing fuel shortages across the East Coast. Ransomware attacks on hospitals have put patients' lives at risk. We heard yesterday about Facebook going offline globally due to faulty configuration. There's word out this morning that Amazon may be facing its own situation today. So part of the problem is that we live in a more connected world. And what we know now is that when there is a data breach, that consumers are the ones that pay the heavy price.

We do not have enough on the books and a federal standard to make sure that companies are more accountable to these breaches. Senator Wicker and I both introduced legislation trying to set a federal data security standard in the United States. We agree that we need to monitor these systems for threats and vulnerabilities, patch their system software's when they needed updates, make individuals who serve as data privacy officers to be more efficient in their oversight, and we agree that the Federal Trade Commission should enforce these standards along with Attorney Generals.

We believe that these companies don't invest enough for the fact that they have oversight to our precious data and information. So we need to act. Massive amounts of personal data are collected from Americans every day as they go online to connect with family, pay bills, work, obtain medical information, send their kids to school, and yesterday was an example of the data that was being collected on children and the offense that we all took to that information and data. Data is collected on Americans whether they like it or not. And we all know stories of data brokers and the breaches behind the scenes where data was collected without anybody's actual acquiescence to that.

So today, Mr. Lee, who is with the Identity Theft Research Center, a nonprofit organization dedicated to helping identity theft victims, will be testifying and according to the ITRC third quarter 2021 breach analysis report, we will again see a record year of breaches in the United States and that these tactics are putting people in greater risk. That's very concerning to me in the state of Washington where in 2020, we saw seven times the rate of identity theft complaints to the FTC over 2019. So this means the 2021 is going to continue to have an even larger number. Hackers are specifically targeting data like logins and passwords and often reuse them across multiple accounts, unlock access to accounts, and cybercrime is lucrative and the data breaches that we are seeing, not only as I said, compromise our data, but are now a big business of cyber and ransomware attacks.

The number of reported data breaches in the first nine months of 2021 exceeded last year's 12 month by 17%. So the numbers keep rising and we're on to another record breaking year. About 116 million individuals have their data compromised from July of this year to September [2021]. There have been more ransomware attacks in the first nine months of 2021 than in both 2019 and 2020. And the number of cyber-attacks so far this year has already surpassed the total number of all data compromises in the year of 2020. So these intrusions take a real toll on people.

Last year, the state of Washington was swept with an insurance fraud as related to unemployment benefits. Later in the year, the Washington State Auditor's Office, which had been receiving unemployment fraud claim had its data compromised due to that vulnerability in the legacy system that was provided by third party. Accellion systems were breached throughout the country, and we still don't know the extent of that breach. But in Washington, the personal information of 1.6 million residents was stolen.

So we know that the identity theft can have a devastating impact on individuals who can't obtain unemployment benefits because a criminal has already applied for them. 40% of these victims were not able to pay their bills. 14% were evicted for not paying rent, 33% did not have enough money for food and utilities, 13% were not able to get a job. So while most identity theft victims lose less than $500, 21% of these victims report losing more than $20,000. And these are a lot of people growing every year in numbers.

So we need to act [to have a better national standard for data security], to protect Americans personal data and privacy, so they're less risk. That's why we introduced the Consumer Online Privacy Act, COPRA, last Congress along with my colleagues here on the committee, Senator Schatz, Klobuchar, and Markey, and continue to grow and strengthen our federal statutes so we can address these issues.

So we look forward to hearing from the witnesses today about those particulars on how we strengthen these standards. What we need to do to protect whistleblowers, what we need to do to report data security and privacy problems. And what we can do to better protect the public. We know that a stronger FTC will help, but we need to give the FTC the resources that they need to do their job. So I again will introduce the witnesses in a few moments, but I think we have a very distinguished panel here to hear from on these important issues.

Question and Answer with the Witnesses

[AUDIO] [VIDEO]

Cantwell: Thank you. Thank you for all the testimony today I want to do as we did at our last hearing, try to figure out whether we have a lot of commonality. So if you could just kind of be brief on answers if you could. Do you all support an FTC Privacy and Data Security Bureau?

Lee: Yes.

Rich: Yes.

Felten: Yes.

Tummarello: Yes.

Cantwell: Do you support first time penalties? If somebody knows the answer.

Lee: Yes.

Rich: Yes,

Felten: Yes.

Tummarello: Yes, if there are clear rules to the road.

Lee: Same.

Cantwell: On this technology issue, one of the key things, Dr. Felton, is to get a technology workforce at the FTC who understands these issues. Ms. Tummarello is bringing up a point about small businesses, but I venture to guess knowing what I've known about the past cases at the FTC, is that the people who are the breach and privacy violators are those who don't have the workforce within their organizations or understand their responsibility as it relates to data and the threat.

I don't know if Mr. Lee might see the same thing -- juxtaposed to startups who are very sophisticated technology players, because they wouldn't be in that business if they weren't very sophisticated technology players.

So what we're seeing is an absence of technology expertise at these firms. Is that correct? The ones that are getting the violations. And Ms. Rich, you can join in here, too. Is that what we saw at the FTC?

Rich: I wouldn't totally agree with that. Sometimes that was the case. But sometimes it was simply a failure to prioritize it, or put the investment there.

Cantwell: That's exactly my point. Yes, companies have a lot of data. And then they don't prioritize, which I consider somewhat being sophisticated with that level of data. So that is the point. So that's who was violating the FTC's actions against people, were people who weren't taking that responsibility seriously.

Rich: Exactly.

Felten: Yes, often, it's a failure to take sufficient care, meaning not recruiting the technology people you need, not managing them carefully, not making this an issue that is on the radar of senior officials in the company. That's what leads to sloppiness and corner cutting, which ultimately, is the cause of a lot of these problems.

Cantwell: So Mr. Lee, your reports show that we had a hearing more than a year ago about Equifax and its breach which was simply not applying a patch that was a known solution. But you're saying we're beyond that even, we're beyond the people just not doing patches, because now the tax, because people understand the amount of money and resources here are much more sophisticated.

Lee: We've gone from a period of data acquisition. So let's think of Equifax was sort of the high point where bad guys wanted to accumulate as much data as they could from as many sources

as they could find. Now we're into a period where they're using the data they've already stolen. So we've gone from a period of theft to a period of fraud. So a lot of what you're seeing in the last year has been circumstances where they'll use that to either perpetrate a phishing, a phishing attack that can lead to ransomware, can lead to that kind of information when you have a login and password from an organization that can lead directly into a ransomware attack because they don't need to breach your system, they can go in with a login and password.

Or you have what you saw with unemployment, where you can pretend to be individuals, and open up accounts, or takeover accounts. So we've gone from acquisition to fraud. Now that doesn't mean they're not still trying to acquire and they're not still using our own tools against us. We don't patch fast enough. We have a legacy software that hasn't been updated or replaced, in some cases, decades. But certainly, you have a lot of legacy software out there in organizations. It's time consuming, it's expensive. I understand that. But it still has to be done. And that leads to the attacks like what you saw at Accellion.

Cantwell: So Dr. Felten, what do you need to require of the companies as relates to the level of technical sophistication that they should have in dealing if they are, let's just say dealing with large volumes of public content?

Felten: Yeah, the bar is certainly higher for them, [it] needs to be higher for them than it has been because the threat is higher. It requires staff, it requires especially sophisticated and strategic approach to managing these systems. And it requires consistent execution. Companies need to be willing to, in some cases, spend money, in some cases, encounter inconvenience to upgrade legacy systems and so on, in order to protect things because what the community has learned over and over is that a single failure to patch one thing, or to upgrade something when it needs to be there to make sure that some digital door is locked, can lead to a huge breach.

Question and Answer, Second Round

[AUDIO] [VIDEO]

Cantwell: Thank you, Senator Rosen, thank you for that line of questioning. I know we have several other members who still want to ask questions that are on their way from the vote. So I'm just going to ask a second round while we're waiting for those Senators to show up. And then hopefully, you guys can go on your way. I know it's been a long morning already. And I know it is a little chilly in here. I wanted to go back to Senator Cruz's question. You know, he was asking about other federal agencies and our own data security issues. And I know now, a couple of members have had discussions with you around NIST. So one, why isn't the FTC just good guidance for the rest of the federal government as it relates to data security?

I mean, I look at NIST as a standard setting, but they're certainly not the policemen on the beat. And we're not asking the FTC to be the policeman on the beat for all of the federal government. But I guarantee you, you're definitely not going to get that out of NIST. So here we have this

burgeoning issue of cybersecurity, for us as a nation, and we need to build our own capacity. We need to build the capacity of a very technical, skilled team. And if you ask me, I have found that there are people in the bowels of organizations who are very, very technical. And then I know people at the very high ends of operations and various aspects of the federal government who are also very knowledgeable and very technical. But I see a gulf of people in between who aren't. And that's the most frustrating thing. So could the FTC, I mean, what do you see this role? Are you back to this notion of, "We're just gonna have to find somebody else to be the government enforcer here to make sure that agencies are doing the oversight?"

Rich: I think what I meant wasn't that the FTC can't provide guidance. In fact, the FTC has been brought in by OPM and OMB to help when there have been breaches to deal with the aftermath, because of the expertise. But, so I think the FTC could work with NIST to provide guidance for the federal government, and there may be others, you know, cybersecurity folks that would participate in that too. What the FTC can't do is make the other agencies follow it, because it's just a lateral agency. And I was in the trenches long enough with squabbles between the agencies, and Ed too, to know that that's just not workable. But the FTC could certainly help provide leadership and guidance that OMB could then push down to the agencies.

Cantwell: Okay. Anything else, Dr. Felten on that? So another point that was brought up, so Miss Rich, on when consumers have been harmed, you believe in their common law rights to sue and to have damages, correct?

Rich: I generally do believe that, absolutely. But I'm speaking, you know, practically about…because it's been such an intractable issue that if you have a really strong law, sufficient resources to enforce it, 50 state AG's on the beat too, that that would be a very good outcome, much better than we have now. And could mean that we don't need to have a private right of action, especially since private rights of action can complicate an already complicated issue.

Cantwell: Well, I would beg to differ on that, from a global perspective, I think yesterday was a perfect example of how you can, if you don't have real damages, that someone is going to feel in these situations, you're going to have a lot of behavior that just continues. And just like on the data security side here, we again, Mr. Lee has been very crisp and clear about the amount of damage that's being done to consumers. But when you think about these organizations across the board, they're not paying the price. I guarantee you that Equifax had nowhere near the damage done to it as the individuals did if you were looking at it in a comparison. I mean, when people lost their homes, lost their jobs, lost their health care, lost these things, it's been pretty significant. So I would just hope that we'll certainly get to you with some you know, questions about what you meant and on those middle ground issues, but I'm going to turn to my colleague, Senator Peters.

Question and Answer, Third Round + Closing Remarks

[AUDIO] [VIDEO]

Cantwell: I wanted to ask you Ms. Rich on your testimony, written testimony. I'm not sure if you mentioned it in your oral testimony. You were talking about common carriers being under the FTC instead of the FCC. Would you elaborate on that?

Rich: Well, I didn't say instead, I didn't say that.

Cantwell: On privacy and data.

Rich: But I do believe that it would be important to create a level playing field, both for consumers and for businesses if you have a data security law. And so for that reason, covering nonprofits and common carriers, and allowing the FTC with the new resources you're giving it, to bring enforcement would be very important. As to the FCC, I don't think they've been particularly active in the data security area. I mean, if you were going to switch it over, I'd have to look at a provision and you know, see whether it would reduce any protections that exists now. But I don't think this has been an area where the FCC has been active or has particular expertise. I think the FTC could do an amazing job with the resources you're going to give it on data security. And the authority you're going to give it on data security.

Cantwell: Dr. Felten?

Felten: I agree the FCC is good at what they do. But I think having that level playing field and allowing the FTC to not face these sort of artificial boundaries in how it does enforcement would be valuable.

Cantwell: Mr. Lee, did you have any comment on this point? I know it might not be your area. But you might have seen cases in here. No? Okay.

Lee: Nope.

Cantwell: All right.

Lee: Thanks for asking though.

Cantwell: Thank you.

Rich: Could you give me 30 seconds to just address the private right of action again? Because I think you think I don't care about consumers and their rights. My point was just that with the proper resources and authority, the FTC, and the states could also represent consumers and get money back for them. Redress, civil penalties, whatever is appropriate. If the law is strong enough, and it gives the remedies. That was my point.

Cantwell: So again, not to put words in your mouth, but you're saying yes, if consumers are harmed, they should be able to get actual damages. The question is, what process should they be able to get actual damages?

Rich: Yes.

Cantwell: And so I think that is going to be a big discussion point among us as well. And so I really appreciate your input on it. Yeah. But I just didn't think that you didn't, I just wanted to make clear that this actually is the issue. And when you look at yesterday, in my opinion, you look at how do you create bright lines within big organizations? How do you have out there in the public and within these companies? Because you don't have a CFO or CTO or even the general counsel, running around every day saying “These are the do's and don'ts”. But you do if there is a strong law, and you know that the company can be held accountable for it. That's the kind of thing we're looking for. And we have to build in as my colleague, Senator Klobuchar, was saying, this is like an entire growth area of our economy. And we want it to succeed, I sit here and listen to it.

There are a lot of good algorithms, trust me a lot of, there are a lot of algorithms that are helping us even today. So yes, now we have a lot of people who are going to understand what algorithms are all about. But the point is, we have to have some bright lines here. And as much as I want a powerful FTC, I think that Europe still fails to get the job done. We kind of know what that looks like. We can see what the European model is accomplishing. And we can see that it has shortcomings. So we know this that, as Mr. Lee was saying, that if you can have these people be accountable to the damage, the same kind of damage that's being done to consumers, you're going to get a better response in policing them. And the Information Age is going to continue to change. So this committee has been very prescriptive, I would say for 15, the amount of time I've been on this committee, very prescriptive. So that's where it's gotten us.

So the Information Age is growing by leaps and bounds in each little sector. We've tried to be prescriptive, and I would say, have we accomplished what we've wanted to accomplish? I would say no, given Mr. Lee's data, and given what we just had yesterday. I would say we need something stronger. We need a very bright line on accountability. But anyway, we'll get to this discussion with our colleagues and hopefully, I think the one thing people who've been watching these hearings will see is that we have a very engaged committee. And it doesn't matter how many cameras are outside that door, okay? Because you had a lot of people here, a lot of people last week asking and knowing the subject area. They are drafting or have drafted legislation in this area. Practically every member of the committee has been on one form or another of this legislation. So I do think the moment is here.

And again, just thank you all for your expertise. This is very, very helpful. And I think that hopefully our colleagues will come together at this moment and, and we'll be able to get some legislation to help bolster and protect consumers. So with that the hearing record will remain open for one week until October 13, 2021. Any Senators who'd like to submit questions for the

record should do so by that date. We ask that responses be returned to the committee as quickly as possible, but no later than August 27, 2021. So with that, the hearing is concluded.