MARSHAL: All rise. Oyez, oyez, oyez. Those persons having business before the Honorable, the United States Court of Appeals for the 12th Circuit, are admonished to draw near and give your attention, for the Court is now sitting. God save the United States and this Honorable Court.

CHIEF JUDGE HOWARD: Please be seated. Well, we have a full house. Does the crier have any further announcements? Then, let's proceed with the appellants on the first issue. Welcome, Mr. Dickman. Whenever you're ready.

HENRY DICKMAN: Mr. Chief Judge, may it please the court. My name is Henry Dickman, and together with my co-counsel Megan Merz, we represent the appellant defendant in this case, Justice Connect. Justice Connect seeks the reversal of the district court's orders in full. I'll be handling the issue of Article III standing for the negligence claim, and my co-counsel will address the Video Privacy Protection Act claim.

The plaintiffs do not have standing, because they cannot carry their burden to establish injury in fact, which is the first and foremost of standing's three elements. What we have here, your honors, is a case of threatened injury, where plaintiffs allege a harm that they expect to happen, not one that has already happened. And in these threatened injury cases, the Supreme Court has made clear that the bar to standing is high. And that's because courts generally should not be deciding cases where an actual injury never ends up occurring.

In *Clapper vs. Amnesty International,* the Supreme Court clarified that a future harm must be certainly impending, or must pose a substantial risk in order to confer standing. But an objectively reasonable likelihood of harm is not sufficient. And if a plaintiff cannot meet those standards, then if and when actual injury does materialize, then a plaintiff can sue at that point.

But your honors, plaintiffs do not meet *Clapper's* demanding standards. And that's so for a couple of reasons. First, as a general matter, data breaches often do not culminate in identity theft, which is the real harm at stake here. Our brief cites empirical studies showing that only about one in five data breaches ever--

CHIEF JUDGE HOWARD: So you're going to talk about substantial risk, I take it?

HENRY DICKMAN: Substantial risk and certainly impending, those are the standards set forth by *Clapper,* your

honor.

CHIEF JUDGE HOWARD: Well, can you help me out? If you're talking about one in five, you know there are some games of chance and other chance-y operations where one in five is not very good odds, it would seem to me-- especially when there are things that are at stake, the kinds of things that might be at stake. And identity theft might be one of those items that there really is a lot at stake. And so, I don't quite understand the 8th Circuit's position that 33% actually coming to fruition is low risk. It just doesn't fit for me.

And I was wondering if there is some connection between certainly impending, whatever that means, and substantial risk-- if that's on a continuum, or if those are entirely separate concepts, and you're going to leave one to the side. Can you help me with what the Supreme Court has been talking about with those two terms?

HENRY DICKMAN: Yes, Chief Judge Howard. A couple points there-- first of all, in footnote 5 of the *Clapper* opinion, the Supreme Court basically treats certainly impending as being synonymous with substantial risk. Those two phrases were carry overs from previous Supreme Court decisions. And in that footnote, they clarified that they basically mean the same thing. And what *Clapper* really is directing courts to do in these situations, your honor, is to look at the chain of intervening causes that must take place between where we stand now and the harm that is ultimately alleged to occur. And the more of those causes there are, and the less likely that any one of those causes is to ultimately materialize, well that suggests that the future harm that is alleged is in fact not certainly impending.

And so our brief lays out the five steps that, in this case, need to occur in order for a harm to materialize. Plaintiffs have simply invited this court to assume that a harm is certainly impending. Their quote is that, "the only event left to occur is the identity theft itself." But this makes the same mistake as the *Clapper* plaintiffs in ignoring that series of intervening causes that necessarily exists between where we stand now and the identity theft, which may or may not occur. And I'd like to highlight a couple of those steps in that causation chain.

So one is the imminence requirement. Plaintiffs must allege a harm to occur imminently, not a harm that will someday happen. And what's important to note about this case, your honor, is that at least nine months have passed since the data breach occurred. And in that time, there has not been a single identity theft committed against not only any class member, in this case, but any Justice Connect premium subscriber at all.

JUDGE NATHAN: If there were an instance now-- maybe even since the district court issued its decision of a single instance of identity theft-- would that be sufficient to provide standing for the class?

HENRY DICKMAN: Well your honor, I think that certainly is a closer case than this one. But ultimately, I would still say no. The fact that one person has been injured suggests that maybe some steps in the attenuation chain are, in fact, not contingent, that they're real.

CHIEF JUDGE HOWARD: So if one person had their identity stolen before the complaint was filed-- and it's determined at the pleading stage, I take it? Standing?

HENRY DICKMAN: Yes, your honor. It is determined at the pleading stage.

JUDGE NATHAN: So we're talking about allegations of a substantial risk. No more than that, right?

HENRY DICKMAN: Yes, your honor. I think what's important to note here is that when we look at this chain of attenuated causes, as more people are harmed, that seems to suggest that the harm that is feared is in fact not that highly attenuated. But in this case, we don't have anyone who is harmed, which suggests that these steps that have yet to occur may be unlikely to ever occur at all.

JUDGE NATHAN: But to help us figure out the boundaries of what is a sufficient risk-- and again, at the pleading stage-- you're saying one would not be enough. How would we evaluate what would be sufficient under your standard? Is it a percentage of the class? And at base, are you arguing that actual harm is necessary in order to establish a substantial risk of harm?

HENRY DICKMAN: So to your second point Judge Nathan, I think that in cases like a data breach-- in the context of credit card fraud-- it is important to see actual harms that have befallen certain people in the class before other similarly situated individuals, who have not yet been harmed, can claim standing on the basis of threatened injury. And that is the case, because as I mentioned at the beginning, data breaches in the context of credit card fraud are unlikely, as a general matter, to result in the harm of identity theft. If this were a completely different situation outside of the data breach context-- whereas a general matter, when event a happens, harm b ensues-- then perhaps in that context--

CHIEF JUDGE HOWARD: I don't understand your point. Your brief cites one empirical study that says 19% result in the kind of injury you're talking about, identity theft. And I think the other study said 22% I'll grant that the facts weren't necessarily the same in the studies, but how is that not substantial?

HENRY DICKMAN: Well your honor, I think the important point--

CHIEF JUDGE HOWARD: Are you just doing a proportionality analysis? I mean, what are you doing?

HENRY DICKMAN: Well your honor, *Clapper* makes clear that there are no hard and fast rules when it comes to these standing cases. *Clapper* says that imminence is an elastic concept. And so, this is necessarily going to be a case by case determination. And circuits on opposite sides of the split have recognized this, that part of what's going to be important is evidence of what has happened so far. Also what's important is going to be the type of information that was breached.

So for example, when we look at the information that was breached in this case, we have names, email addresses addresses, phone numbers, and credit card information. Well, the primary financial harm that is presented by that breach is credit card fraud. And this presents a different set of harms than if information like social security numbers or dates of birth had been stolen.

JUDGE OLDHAM: So why does it matter that the first link in your chain of five links is that the hackers have to be motivated by a purpose to misuse the information? I'm not sure I understand why that link is there, even if you agree with the other four. Because one, the fact that the data was breached itself is an increase. We can argue about whether it's a substantial risk, but it's certainly an increase of threatened harm.

And two, regardless of the purpose of the original breach, the back end purpose of what to be done with the information doesn't seem to be motivated by the purpose on the front end, if that makes sense. So you could imagine hackers hacking the information and then using it for a different purpose once they figured out what they got. So I'm not sure I understand why it matters what their purpose was in originally taking the information.

HENRY DICKMAN: Well your honors, the hacker who has the information has to have a financial motivation. So there might be a variety of other motivations that a hacker might have, and our brief lists some of those. It might be a foreign nation with an espionage related intent. It might be a hacktivist with an ideological intent.

JUDGE OLDHAM: What if it's just a hacker that tries to get access to the database, just to get it? Either to show that the database can be breached-- you read stories about this in the newspaper every day.

It would obviate the first link in the chain.

HENRY DICKMAN: Well your honor, respectfully, I would argue the opposite, which is that if a hacker doesn't have any intent to actually do anything with that data but simply wants to hack for the sake of hacking, then no harm will ever ultimately result. The hacker in question must have some kind of motivation to commit financial harm. And if that hacker doesn't have that motivation, then the harm that plaintiffs fear in this case-- which is identity theft-- will never ultimately ensue.

JUDGE OLDHAM: What if the hacker's purpose in breaching the database is to sell the information to somebody else?

HENRY DICKMAN: Well your honor, that certainly could be the case. But that is yet another link in our chain of attenuating causes. In fact your honor--

JUDGE NATHAN: How do we know what the intent of the hacker is? And just to put it in procedural terms, again, this is a motion to dismiss. So we take the allegations and the complaint on face value. You do a lot of citation to, what I think are, extra record materials, trying to establish a minimal risk. Why is that appropriate to consider at this stage?

HENRY DICKMAN: Well Judge Nathan, I think what's important here is figuring out whether or not the harm that is alleged is certainly impending. And we have to look at what usually happens in these kinds of cases. And the fact of the matter is that in the context of these data breach cases, identity theft sometimes occurs. And more often than not, it does not occur. And this attenuation chain gives great evidence for why that is the case. So another step in this chain--

CHIEF JUDGE HOWARD: Before you go there, please answer Judge Nathan's question.

HENRY DICKMAN: I'm sorry, Judge Nathan. What part of the question?

JUDGE NATHAN: Just the procedural question. So we take the allegations and the complaint at face value. It seemed to be true.

HENRY DICKMAN: Yes.

JUDGE NATHAN: And in making your point about the unlikelihood of hacking, you cite to a lot of extra record website information. I don't know where it came from or what good it is. Why is that appropriate on a motion to dismiss, where what matters for purposes of standing here at this

stage are the allegations and the complaint?

HENRY DICKMAN: Yes. So your honor, the allegations in the pleading stage are to be assumed as true in the context of what has already happened. So when alleging, for example, that there was a data breach and this is the information that was contained in that data breach, that's assumed as true. And we don't dispute that. But we don't necessarily take as given the plaintiffs' allegations of what's going to happen in the future. If that were the case, then--

JUDGE NATHAN: Isn't it a factual question, this question of ultimately substantial risk? You're citing factual material to us to make the assessment.

HENRY DICKMAN: It is a factual question, your honor. But whether or not the circumstances that have occurred in the past will ultimately result in the harm that is alleged to occur in the future depends on a variety of other things happening in the real world that have yet to happen and that can't be alleged as having already happened.

One of those is the hacker's intent. Another is whether or not the hacker will try to commit identity theft imminently. Another is whether or not the hacker will ultimately be successful in committing identity theft. And in the context of credit cards, that seems particularly questionable. And that's because if a credit card company finds out about this breach, then in many cases, they will simply deactivate the credit card. And at that point, the information that the hacker has is worthless. And he will be unable to commit identity theft.

And yet another step in the chain, and this is perhaps most important, is that even if everything plaintiffs fear occurs-- which is that a hacker takes this credit card information and misuses it for their own financial gain-- the plaintiff is still unlikely to be injured. And that's for two reasons. One, federal law requires that when a cardholder's credit card information is misused but not the card itself-- which would be this case-- that a credit card company cannot hold the cardholder liable for those fraudulent charges.

And second, all four major credit card companies-- MasterCard, Visa, American Express, Discover-- they have all contractually agreed to not impose liability on cardholders whose information has been fraudulently misused. And so your honors, when we look at what *Clapper* commands-- which is to examine this chain of attenuated causes-- and we think about the situation that we have in front of us here, we see that the harm is highly attenuated and that the harm that plaintiffs fear--

CHIEF JUDGE HOWARD: I'd like to just follow up on your last point, though, before you continue. One of the other items that you mentioned was that a person could protect themselves by putting on a credit freeze, locking their credit. But your brief doesn't talk about the cost that's associated with that. Do you have any idea what it means to a person when they actually go through a credit freeze? And if you do, tell me why that's not injury itself.

HENRY DICKMAN: My time has expired. May I have leave to answer the question?

CHIEF JUDGE HOWARD: Of course.

HENRY DICKMAN: First of all, Judge Howard, plaintiffs have not alleged any kind of actual expenses already incurred, such as time spent on a credit freeze. And moreover, a credit freeze is a more serious measure than what needs to be taken in this case. Credit freezes are--

CHIEF JUDGE HOWARD: But you briefed the issue. You said that's one of the options that they have.

HENRY DICKMAN: That's the option that a victim of a data breach generally has. And that would be more applicable in the case of a breach which included social security numbers or dates of birth. But in this case, all we have is a breach of credit card information, which makes the harm even more attenuated than the social security number cases. And a plaintiff can simply call their credit card company and deactivate the card.

JUDGE NATHAN: So is it your position that no breach of credit card information would ever be sufficient to establish standing? It sounds like you're saying given that credit card companies are going to cover the costs, and you can put on a credit freeze, it really doesn't matter if hundreds of people in this class had experienced credit card fraud as a result. Right? That wouldn't establish standing. The causal chain would be broken in your position.

HENRY DICKMAN: So Judge Nathan, I think there are some actual harms that can result from credit card fraud. So for example, if someone were out of the country and this happened, and they experienced a hold on their credit card because of the fraudulent charges and were unable to get money, that seems like a situation where a plaintiff could plausibly allege harm on the basis of credit card fraud. If they do have to spend many hours on the phone with their credit card company trying to sort out a fraudulent charge, that might be the basis for harm. But we don't have any of those things alleged in this case. The record makes clear that no one has incurred

monetary damages to date. Your honors, it's for all these reasons that we ask that this court dismiss the negligence claim for lack of standing. Thank you.

CHIEF JUDGE HOWARD: Thank you.

JUDGE NATHAN: Thank you.

KATHERINE WHISENHUNT: May it please the court. My name is Katherine Whisenhunt. And I, along with my co-counsel Abby Thornhill, represent the appellee, Miss Yasmine Surry. Miss Surry respectfully requests that this court affirm the decision of the district court in full. I will address why Surry has constitutional standing to sue, and my co-counsel will address why Justice Connect violated the Video Privacy Protection Act.

Miss Surry has constitutional standing to sue, because she has plausibly alleged an injury in fact sufficient to satisfy the substantial risk standards set forth by the Supreme Court in *Clapper.* This court should hold that the increased risk of identity theft following a data breach is a substantial risk, because the purpose of accessing sensitive information through a breach is actual misuse. And the risk that follows is neither speculative nor attenuated. Beginning with the purpose of hacking--

CHIEF JUDGE HOWARD: Do you agree with your friends on the other side that substantial risk means the same thing as certainly impending in the Supreme Court's view?

KATHERINE WHISENHUNT: No, your honor. I would not agree with that statement given the Supreme Court's decision in *Susan B Anthony List,* in which the court clarified that those were two separate ways to establish injury in fact. In *Clapper,* the court stated that a substantial risk which may prompt plaintiffs to reasonably incur costs to avoid or mitigate that harm was sufficient to be an injury in fact.

JUDGE OLDHAM: But wouldn't you need to have the actual costs? I mean, it might be one thing to say that it's a substantial risk if you have to incur the costs. But you still would have to allege that you had incurred the costs, right? To avoid the risk.

KATHERINE WHISENHUNT: No, your honor. Threatened injury under the standard is sufficient. So the plaintiffs here are alleging an increased risk of identity theft following the data breach as the injury in fact. And this, for two reasons, qualifies a data breach, can create this injury in fact. So if we look first to the purpose of hacking, a substantial risk of harm exists when hackers access information

through a breach, because the purpose of hacking is misuse.

The Seventh Circuit found this purpose instructive in *Remijas versus Neiman Marcus.* In that case, the plaintiffs had alleged standing based on the greater susceptibility to identity theft following a hack of Neiman Marcus, in which the hackers stole the plaintiff's credit card information. In that case, the Seventh Circuit found that it was plausible to infer that the plaintiffs had suffered a substantial risk of harm, because presumably, the purpose of that hack was to commit identity theft. The court asked, why else would hackers break into a store's database and steal consumers' private information? Presumably, the purpose of that hack was to misuse the information for identity theft.

Similarly, this court can infer in this case with the pride parent hack that the purpose of the hack was to commit identity theft. The pride parent hacker breached the system, and Surry and other plaintiffs fell victim to this data breach, in which the hackers obtained access to names, email addresses, phone numbers, credit card information, home addresses. Like in *Remijas* with the credit card information, it's plausible for this Court to infer that the purpose of that hack was to commit identity theft.

CHIEF JUDGE HOWARD: Mr. Dickman said that it probably wasn't that motivation, but rather some other form of fraud-- credit card fraud, for example. So, do you have a response to that?

KATHERINE WHISENHUNT: Yes, your honor. Two responses to that-- first, credit card information was stolen in this hack. However, that was not the only type of information stolen. So the plaintiffs can be at risk of other types of identity theft, not merely the credit card information. But I do want to address the other alternative purposes point as well, because although alternative purposes of the hack other than identity theft might not be inconceivable, this does not render implausible the plaintiff's claim that the increased risk of identity theft following the data breach is a substantial risk.

And we can look to the DC circuit decision in the OPM data breach litigation. In that case, the OPM had argued that another plausible or possible motive behind that hack was espionage. And they argued that it was not possible for the plaintiffs to construct a credible theory that the hack was motivated by identity theft. However, the DC circuit rejected that argument. The DC circuit held that even though it was possible for a cyber attack to be motivated by purposes of espionage, it was just as plausible to infer that the hack was motivated, or at least one of the hacker's goals, was identity theft.

JUDGE OLDHAM: What are we to make of the fact that the district court doesn't say any of this? The district court's analysis of the substantial risk of identity theft is one sentence, effectively, that just says well, Justice Connect acknowledged the breach, and said take protective measures to prevent your identity from being disclosed, and acted as if that effectively concedes the injury in fact that your client would need to invoke the jurisdiction of the federal courts. So what do we do with the district court's opinion?

KATHERINE WHISENHUNT: Yes, your honor. I would like to make clear that we're not asking this court to hold that the plaintiffs have standing because of the fact that Justice Connect urged the customers to take remedial measures. Although, that has been a consideration by several courts. We can look to the Ninth Circuit decision in *Zappos* and the Sixth Circuit decision in *Galleria.* However, we're not asking the court to decide solely based on that fact. That is just further evidence that the company does see this as a substantial risk. But rather, this court--

JUDGE NATHAN: Well, it's that they see it as an increased risk. I don't think there's reason to conflate increased risk with substantial risk. Right?

KATHERINE WHISENHUNT: Yes, your honor. That's correct. I don't mean to conflate the two. But they do recognize that this is a risk, or they would not have urged the customers to take those measures. However, this court can look to the fact that the purpose of accessing sensitive information through a breach is actual misuse. And the risk that results from that is neither speculative nor attenuated.

And I want to go a little more into that lack of speculation and attenuation, unless you're asking a question.

JUDGE OLDHAM: No. Please.

KATHERINE WHISENHUNT: Because I think that's important to distinguish from the circumstances in *Clapper.* So in *Clapper,* the Supreme Court held that the risk alleged there, which was that the communications with foreign contacts, would be intercepted under the Foreign Intelligence Surveillance Act. And the court said that the injury in that case was too speculative, because it was based on a highly attenuated chain of possibilities. A series of five events had to occur before the plaintiffs would suffer any harm in that case.

However in contrast, in the context of data breaches, there is no highly attenuated chain of possibilities. The only event left to occur is the actual harm itself. We can look to the DC

circuit's opinion in *Attias* to see this distinction from the circumstances in *Clapper.* So in *Attias,* the DC circuit addressed this issue and said in data breach cases, there's no long sequence of uncertain contingencies involving multiple independent actors that has to occur before the plaintiffs will suffer any harm.

CHIEF JUDGE HOWARD: Was that on a motion to dismiss, or was that a summary judgment after discovery about what actually had gone on?

KATHERINE WHISENHUNT: Your honor, I'm not sure. I'd have to double check that. But either way, the court did look to comparing *Clapper* to the circumstances in a data breach case, finding that there is no long sequence that has to occur.

And I think another important distinction that the DC circuit pointed out was that multiple independent actors were involved in the *Clapper* case. So it involved opinions and decisions to be made by the executive branch intelligence officials and Article III judges serving on the Foreign Intelligence Surveillance Court. So the decision of the next person depended on the decision of the person before them. It was a series of ifs. But in contrast, in data breach cases, it's the hacker themselves who already accesses all of the information.

JUDGE NATHAN: If we have the same facts here, minus the credit card information being hacked, does that impact your argument?

KATHERINE WHISENHUNT: Your honor, I think it would be harder for hackers to use just the rest of the information to commit identity theft. I do still think that there is a risk of identity theft without those credit card information. But given the fact that we do have names, email addresses, phone numbers, home addresses, and the credit card information, that information combined gives the hacker everything that they need to commit the identity theft.

JUDGE OLDHAM: Suppose instead of the communication that Justice Connect sent to your client and the rest of the class they did what other companies sometimes do, which is to say dear customer, your information has been compromised due to an unfortunate breach. But as a consequence, our company is going to pay for one year of identity theft protection insurance. Would you agree with me that would make it impossible, at least on the complaint that your client has filed in this case, to establish Article III injury in fact?

KATHERINE WHISENHUNT: I'm sorry. If they had provided those services, that would make it difficult to establish Article III standing? No, I don't think so, because there's still an increased risk of identity theft following

the breach, even if those services were in place. So this is highly sensitive information that we're talking about here. And hackers can use tactics to even gain more information based on that, such as phishing. So I think there still is an increased risk of identity theft, even if those services were in place.

But I want to touch a little more on that lack of speculation and lack of attenuation in data breach cases.

CHIEF JUDGE HOWARD: Before you do that, just to follow up on this point-- what do you make of the view held by the 8th circuit and perhaps some others that only one third had their identity stolen, and that's not a substantial risk. It doesn't meet the *Clapper* factors?

KATHERINE WHISENHUNT: Your honor, I do think that's a substantial risk. But you know, as we mentioned--

CHIEF JUDGE HOWARD: But why is the 8th circuit wrong?

KATHERINE WHISENHUNT: Your honor, the 8th circuit case was involving only credit card information. So one difference from the case that we have here, it involves more information, including names, email addresses, phone numbers, and those home addresses in addition to the credit card information. But the 8th circuit took an approach that most of the circuits have not taken. The way that the other circuits have addressed this question was not looking to a specific statistic, which could change or still be considered substantial in the views of another court. However, the other circuits have looked at this level of speculation and attenuation, or lack thereof, in comparing the circumstances to those in *Clapper.*

JUDGE NATHAN: Well, how would you say we should measure substantial risk? What guidance should we give the district courts in making that determination, in your view?

KATHERINE WHISENHUNT: Yes, your honor. I think there's two ways to measure that. First, if it's plausible to infer that the purpose of the hack was to commit identity theft. In this case--

JUDGE NATHAN: You agree that's a factual question you'll have to prove, what the intent of the hacker was?

KATHERINE WHISENHUNT: Yes, your honor. But as we have discussed previously here today, the standard is a plausibility standard. It must be plausible to infer that there's a substantial risk. So if identity theft was plausible purpose of the hack, then I think that is satisfied here today and in cases where it's

possible to infer that is the purpose of the hack.

But also, the other thing that this court can look to is the lack of speculation and attenuation. We have a standard from the Supreme Court's case in *Clapper* that threatened injury is sufficient, that a substantial risk of harm-- if the plaintiff can show that-- confers or satisfies the substantial risk--

JUDGE NATHAN: But how do they show it? Just in practicality, what would it look like?

KATHERINE WHISENHUNT: Yes, your honor. So we look to the fact that there is nothing left to occur, that the hackers have possessed all the information that they need. So one helpful distinction might be whether the hackers have accessed the information. And several circuit courts have made this distinction. So if we look to the DC circuit in *Attias* and OPM as well as the Ninth Circuit in *Zappos* and compare those to the 3rd and 4th Circuit's decisions in *Beck* and *Riley*-- in the first list of cases that I mentioned where the courts did find an increased risk of identity theft, there was evidence that the hackers had accessed the information.

In contrast, in the Fourth Circuit case of *Beck* and the Third Circuit case of *Riley,* it was unclear whether the hackers had actually accessed that information. So the Fourth Circuit and the Third Circuit, in those two cases, found that the risk was too speculative, because there was no evidence. Like in *Beck,* there was a stolen laptop. There was no evidence that hacker had actually accessed the information. Similarly in *Riley,* the fact revealed that the hacker potentially accessed the information. So that would be a standard to look to. In this case, we know that the pride parent hacker has accessed that information. But that is something the court could use it to draw that distinction and something that the circuit courts have used thus far.

CHIEF JUDGE HOWARD: Are you saying that there is no circuit split on this particular issue?

KATHERINE WHISENHUNT: No, your honor. There is a circuit split on whether the increased risk of identity theft following a data breach is a substantial risk. I just mean to suggest that the way the courts have addressed whether a risk is substantial or not is looking to that level of speculation or attenuation, comparing it to the circumstances in *Clapper.* And a distinction that has been drawn is whether that information has been actually accessed, whether there's evidence of that access by the hackers.

JUDGE 3: But one of the things in *Clapper* is there were very specific allegations of things that the plaintiffs in that case had in fact incurred. Injuries that, in fact, the plaintiffs had incurred. And the court says these aren't going to be sufficient for various reasons. But one of the reasons they point out to is that you have to prove each of these facts. And it just requires too much speculation from the moment of the filing of the complaint to the point of decision to infer the connection.

And what I'm struggling with in this case is, I don't see the allegation of the injury in fact, whether it's the access of the information, or the use of the information, or the purpose. The only allegation I can see from your client here is the information, that the database was breached. But we know nothing else beyond that, which is why we end up talking about statistics of identity theft.

KATHERINE WHISENHUNT: Yes, your honor. And I think that if we look to several of the court's decisions-- like in the DC circuit case, the OPM data breach litigation-- they said based on the fact that the hackers had accessed that information, the hackers possessed everything that they needed, all of the information they needed to steal the plaintiffs' identities. Similarly, the Ninth Circuit in *Zappos* articulated this lack of speculation, saying that the hackers as a result of that data breach had the means to commit the identity theft.

So I think we can say, based on the fact that they have possession of that information-- they've obtained access, just as the DC circuit stated in *Attias,* it's plausible to infer that the hackers had both the intent and the ability to use that information to commit identity theft. If there's no further questions?

JUDGE NATHAN: Just a parallel procedural question to what I asked your colleague on the other side. Do you think you're done with respect to standing? In other words, you've established it. Or you'll prove it at trial.

KATHERINE WHISENHUNT: Your honor, I believe at this stage in the litigation, we have plausibly alleged a sufficient injury in fact to establish standing. I do recognize, as the Supreme Court stated in *Lujan,* that each element of standing must be shown with the manner and the degree of evidence required at the successive stages of the litigation. So I do recognize that could have to be addressed at a further stage of the litigation. But for these reasons, we respectfully request that this court affirm the decision of the district court. Thank you.

CHIEF JUDGE Thank you. Being new to the 12th circuit, I'm not sure if we go right to rebuttal now or we go to

HOWARD: the second issue. Does anybody know?

JUDGE NATHAN: Second issue.

CHIEF JUDGE HOWARD: Second issue. We'll hear from the appellant. Whenever you're ready.

MEGAN MERZ: Thank you, your honor. May it please the court. My name is Megan Merz, and I represent the appellants in this case, Justice Connect. We agree with appellees that the Video Privacy Protection Act covers more than just facially identifiable information. It covers information that can be used to identify individuals. The question at issue today is from whose perspective must it be identifiable?

Appellees present the so-called game program standard, which asks case by case whether the information disclosed by the recipient can be linked back using other data to the particular individual. We instead ask this court to use the ordinary person standard to determine whether information can be linked back to an individual.

There are three reasons why we should use the ordinary person standard in defining PII, or personally identifiable information. First, only the ordinary person standard retains the statute's textual focus on the disclosing party. Second, only the ordinary person standard is consistent with legislative intent in enacting the VPPA. And third and finally, the ordinary person standard accommodates new technology without turning everything into PII.

First, let's talk about the statute's textual focus on the disclosing party. Enacted in 1988, this statute is framed from the perspective of regulating videotape service providers. Section 27.10 expressly prohibits providers from knowingly disclosing PII concerning any consumer under the threat of punitive damages. The text does not mention the recipient, nor does it place any punitive damages--

JUDGE NATHAN: Well, doesn't it? Doesn't it say to any person? Just looking at the text, videotape service provider who knowingly discloses to any person. You want "any" to mean something other than any, right?

MEGAN MERZ: Well I think, your honor, the focus of the text is still on the information in the disclosing party. And the actual punitive damages lie on the disclosing party. There are no implications for the recipient who receives that data. But I think that the game program standard shifts the focus of

that statue to the receiving party and what they're capable of doing.

JUDGE NATHAN: You do essentially want us to read that as to any non sophisticated person, or to any ordinary person rather than any person.

MEGAN MERZ: Well I think, your honor, if it were any information that could possibly identify anyone to any person, released to any person, that standard would be impossibly broad. And I think that's actually broader than the standard appellees are arguing for. Theirs is recipient based, so it's only the particular recipient who is receiving the information, whether they can trace that back to the individual. So I don't think either side really believes that any person is the relevant actor here. I think there has to be a limiting principle for what is identifiable and to whom identifiable applies. We think the ordinary person standard serves the purposes and fits the text of the statute.

CHIEF JUDGE HOWARD: Why wouldn't the limiting principle be something like, you've decided to enter the marketplace and engage in the business of selling this information to people who are going to use it for what they used it for. And why can't that be taken in context with respect to focusing on the disclosing person?

MEGAN MERZ: Well I do think, your honor, that when Congress wrote the statute-- by virtue of writing in personally identifiable information, Congress envisioned that it was carving out a narrow swath of information. This wasn't a statute that was applying to all information. So to answer your question, I think Congress assumed that video providers would be able to disclose some category of information without incurring liability under this statute, by virtue of setting aside a particular category of information.

And I think that's where the argument arises that the game program standard turns essentially everything into PII and writes out--

CHIEF JUDGE HOWARD: But if you know when you sell the information that the recipient has the ability to identify the person, why should you be let off the hook? Why does the statute not apply to you in that circumstance?

MEGAN MERZ: Well I think, your honor, that in that circumstance, it becomes a case by case adjudication. So in each instance, that piece of information could be PII or could not be PII. It takes the focus away from the information that's actually regulated by the statute and puts it on who the recipient is. So maybe an example might clarify.

CHIEF JUDGE HOWARD: I'm suggesting that it puts it on the discloser. It just puts it in context. I'll take your point that it takes the emphasis off the information. So what do you do with that?

MEGAN MERZ: So your honor, I think it also places an enormous burden on the actual provider. So when Congress was discussing this statute, they were balancing two interests. One, we agree with appellees, was the interest of privacy. But Congress also had a stated interest in not over penalizing videotape service providers. In fact, Congress specifically--

CHIEF JUDGE HOWARD: Do you think that there was an intent to incentivize selling of this information?

MEGAN MERZ: I don't think there was necessarily an intent to incentivize it. But I don't think--

CHIEF JUDGE HOWARD: But your position does that.

MEGAN MERZ: Well, I don't think Congress envisioned that all information would be considered PII. I don't think Congress thought that any single piece of information that a videotape service provider sells could be considered PII under this statute. I think by virtue of writing a specific category for personally identifiable information, that demonstrates Congress didn't just view this as all information. So I think whatever our opinions are on what companies should or shouldn't do, I think the scope of this statute means Congress envisioned companies being able to release some data without being subject to punitive damages under this statute.

JUDGE 3: Isn't the key textual word, though, identifiable? Your friends on the other side make quite a point about the fact that it's not personal identity information. It's not just, you know, things that actually disclose the identity of the customer. It's identifiable. And it would make some sense that the statute therefore imposes on your client the responsibility to determine what's identifiable. And if the stuff is identifiable to any person, then it would fall within the scope of the textual provision, I would think.

MEGAN MERZ: I think I agree in part, your honor. We agree with appellees that this statute goes beyond just identity information, someone's name essentially. It goes beyond that, and I think identifiable implies that it extends to information that can be used to identify someone. I think that brings it back to that initial question I started with, which is whose perspective must it be identifiable from? And I think when you make it about the recipient, I think that has enormous implications that don't fit with what the statute was intended.

I think it's also worth noting what the statute was written in the context of, when it was first written, which was when Judge Bork's video rentals were released to the public. Congress was talking about this in the context of someone being publicly humiliated-- their name, their identity being tied to their particular taste in videos.

JUDGE NATHAN: So is your position that it is limited to names?

MEGAN MERZ: No, your honor. It's not at all. We think it's limited to things that an ordinary person could readily link back to an individual. So an example of that accommodating technology might be a phone number. So we think in 1988, a phone number probably would not have counted as PII. We think today, if you type in a phone number into Google, usually you're going to get someone's full name on the first page of Google. That today, under our standard, counts as PII.

JUDGE NATHAN: So context does matter?

MEGAN MERZ: Context matters, your honor. We don't think this is an impossibly rigid standard. But we also don't think that we can swing entirely in the other direction and open this up so that all information is essentially counted as PII, which more or less renders the text of the statute moot.

Now, our colleagues actually bring up multiple other statutes that we think further clarify congressional intent on this point. CAPA is one example. HIPAA is another. These are other statutes that specifically write in things like device identifiers, or they delegate power to the FTC to expand over time the definition of PII. And I think it's notable that this statute--

JUDGE NATHAN: But you think the definition does expand over time. You just said, a phone number back then, no. Now, yes. So it does. It does change over time depending on available technology.

MEGAN MERZ: Yes, your honor. We think it does. But there's no agency that's delegated the power to explicitly change what is included within PII over time. And that's what CAPA does, which I think both of our briefs actually cite. So those statutes are written with the language PII in them. But completely different language is used to define PII, and I think that demonstrates Congress knows how to write a statute that defines PII in the way that appellees contest. But Congress didn't do that in this statute.

JUDGE 3: But Congress also knows how to write a statute that allows companies to sell to advertisers

this sort of partially anonymized or fully anonymized data, as they have done for example in the telecommunications context. So doesn't the inference cut the other way, at least in that part?

MEGAN MERZ: Well I do think, your honor, it's worth noting this was enacted in 1988. So a lot of the technological telecommunication space didn't look the way then that it looks now. But even so, I will say Congress did revisit this in 2013. And a prominent amicus brought up that things like digital identifiers aren't included in the statute as it stands. So they were presented and notified of kind of a modern take that appellees provide on what the statute could be adopted to mean. Congress ignored that and didn't change the statute at all.

JUDGE NATHAN: Because they thought it already encompassed it.

MEGAN MERZ: We don't think so, your honor. We think they envisioned more the scenario that aligned with what they enacted it in reaction to, which was that of Judge Bork being publicly humiliated. We also think that adopting the game program standard effectively creates absurd results that Congress would not want to get behind. Just based on the broad swath of information that would be swept up and, again, rendering the text of the statute roughly moot.

JUDGE NATHAN: We understand what falls within your test. You've said names, phone numbers. Yes?

MEGAN MERZ: Yes, your honor.

JUDGE NATHAN: Addresses?

MEGAN MERZ: Most likely, your honor. Yes.

JUDGE NATHAN: Social security numbers?

MEGAN MERZ: We don't think so, your honor. We actually don't think social security numbers fall under the ordinary person standard. They're not something that, if I read it out in this courtroom, someone could link back to an individual. That's not to dismiss the importance of social security number disclosure, of course. But we think that there are other regulatory schemes out there to protect that type of data. Even privacy torts might protect that type of data. Moreover, the statute was written in the context of companies like Blockbuster or Hulu, which are largely unlikely to possess people's social security numbers. So we think at the point that Congress wasn't thinking about that when they wrote it, and at the point that there are other regulatory frameworks to protect things like social security numbers. We don't see a problem

with the fact that the ordinary person standard doesn't cover those.

JUDGE NATHAN: You said yes to addresses.

MEGAN MERZ: Yes, your honor. Most likely.

JUDGE NATHAN: This here-- factually, doesn't it include location information?

MEGAN MERZ: So yes, your honor. There was a district court finding a fact that in this case, the GPS location data was not precise enough to correspond to someone's address or to be specific enough that an ordinary person could track it back to an individual. So that's something we agree with appellees on. So in this instance, we all agree that this is not information that was disclosed here that can be traced back by an ordinary person. And we think that's the most appropriate and predictable standard.

Even if you look at the context of their standard, it doesn't provide the enormous protections that they claim. For example, a company could disclose a piece of information to a startup that it wouldn't be allowed to disclose to Apple, even if that startup were then to go out and acquire the same information that Apple already has. So it doesn't actually protect consumer privacy in the enormous ways that they contend. But it does create enormous costs for the video providers. It creates an enormous burden, and it potentially rewrites the text of the statute by saying that all information eventually is going to be encompassed as PII.

And we agree with appellees that the ultimate purpose of the statute is largely privacy. But it specifically says in the Senate committee reports that they intended to protect consumer privacy to a reasonable, legitimate, enforceable extent, not to the broadest extent possible.

CHIEF JUDGE HOWARD: What if the limiting principle were simply that the seller of the information has knowledge that the purchaser of the information has a game program and understands how that game program works? Would that be a good cut off?

MEGAN MERZ: I don't think so, your honor, because I do think the game program standard has a reasonably foreseeable aspect. But to some extent, companies are always expected to foresee the types of corporate partners they're dealing with.

CHIEF JUDGE HOWARD: I'm proposing just a little further down the line, actual knowledge.

MEGAN MERZ: I do think, your honor, it still enters the same territory of potentially making everything PII. Even if a company is selling to a company like Apple, most of us can safely assume Apple has a lot of information on all of us. And that company would be expected to foresee almost certainly that Apple can connect something as simple as a zip code back to an individual. But that would then make this statute one that covers the disclosure of any information, again, as simple as the zip code and the movie *Legally Blonde.* That could be enough, as a disclosure, to count as PII under the statute.

JUDGE NATHAN: To Apple. It's limited, because it's saying in light of the information you have about the recipient, how much are you revealing?

MEGAN MERZ: I see my time is expiring. I wonder if I may answer?

CHIEF JUDGE HOWARD: Yes.

MEGAN MERZ: Yes to Apple. But we envision a future in which more and more companies are collecting more and more data. And you see-- and courts have acknowledged this-- you'll see more companies looking like Apple, where they have enormous amounts of data about us. So as we progress in the future, the game program standard becomes increasingly and increasingly unworkable. Even as the burden of figuring out who knows what decreases on the provider, the odds that all of these companies have all this information on us increase. So for all these reasons, Justice Connect requests that this court reverse the grant of summary judgment.

CHIEF JUDGE HOWARD: Counsel, before you step back, I know that *Yershov* was not a 12th circuit case. It was some circuit up in New England if I'm not mistaken.

JUDGE NATHAN: I hear nice things about their Chief Judge.

CHIEF JUDGE HOWARD: You were listening. Do you know if Justice Souter was on that panel?

MEGAN MERZ: I believe he was, your honor.

CHIEF JUDGE HOWARD: Does that change your view of the case at all?

MEGAN MERZ: I don't think so, your honor. We still think that Yershov split from the rest of the circuits in this

instance. And we do think that the rest of the circuits had it right when they applied the ordinary person standard.

CHIEF JUDGE HOWARD: I'm just giving you a hard time here.

MEGAN MERZ: Thank you, your honors.

ABBY THORNHILL: May it please the court. My name is Abby Thornhill, and I represent the appellee Yasmine Surry. Miss Surry asked this court to affirm the decision of the district court and hold that personally identifiable information, as defined by the Video Privacy Protection Act-- the VPPA-- includes information from which both an ordinary person, as well as a sophisticated recipient may identify an individual. Adopting this standard would be consistent with the First Circuit's decision in *Yershov.* And under the First Circuit's test, the appellant Justice Connect is liable for knowingly disclosing personally identifiable information when it sent its consumer preference data to the clothing company.

The court should hold them this way for three main reasons. First, the text of the VPPA is broad and clearly indicates that Congress meant to include all information that is capable of identifying an individual. Second, the First Circuit's test is consistent with the overall purpose of the VPPA to continue to protect personal information in an increasingly intrusive and sophisticated technological world. And third, a broad understanding of personally identifiable information is consistent with the government's use of the phrase, as well as its close equivalents throughout the government's statutes and regulations in the privacy sphere.

But I want to start with the text, because as the Supreme Court has continuously held, any question of statutory interpretation should begin with the text, giving each word its contemporary, ordinary, and common meaning. So first, Section 27.10b creates the general prohibition against videotape service providers disclosing personally identifiable information. But a3 provides the actual definition of personally identifiable information. And that's the text--

JUDGE NATHAN: You don't put any weight in your brief on the inclusion of the to any person language. You think that has no bearing on the question?

ABBY THORNHILL: It potentially adds bearing. However, the First Circuit's decision in *Yershov* focused instead on the actual text of the definition of personally identifiable information-- specifically, first looking at the suffix "able," as Judge Oldham, you noted-- addressing our friends on the other side.

And it is specific there, and it does not specify a specific category of information as the appellants suggest. Instead, it left the term open, leaving it as all identifiable information, all information that is capable of identifying an individual.

Additionally, the text starts with personally identifiable information includes. And I think the First Circuit's discussion of includes is also particularly helpful. So includes first, on its own, suggests that the definition provided is only a minimum. And we have further legislative history that confirms that interpretation. But further, Congress also chose the word includes instead of means, and this is significant because within subsection a-- in the definitions for other terms, such as videotape service provider-- Congress did specifically use the term means to actually define those definitions. Here, we have only that x is an example of y, rather than x is y.

But further-- and I think this is particularly important, because as our friends on the other side suggest, potentially addresses might not be included in personally identifiable information-- we have from the text of section b2d that in fact, they are. So in section b2d of the statute, there's actually an exception to the general prohibition against videotape service providers disclosing this information. And it says that if you first provide an opt out option, but then the only personally identifiable information that's actually disclosed includes names and addresses, there is no liability.

So in saying that solely names and addresses are the type of information that you can disclose, we know that names and addresses first are included within personally identifiable information, but also that they're a minimum. And there's more included under the statute. So as our friends suggest, if addresses potentially do not actually reveal to an ordinary person who is matched with that video content history, then we have a plain inconsistency with the actual text of the statue.

JUDGE NATHAN: So what do you understand to be the limiting principle in the example? The example given is certain companies now have the capability where the zip code with a couple likes is enough to provide the information. So zip codes would be sufficient to trigger this, in your view?

ABBY THORNHILL: So asking particularly if any single piece of information is personally identifiable information isn't exactly the right question. The question is about to whom the party is disclosed. So if zip codes are given to a company like the Chloe Company-- where their entire business model is their ability to aggregate data and particularly identify individuals-- if a zip code would allow them to do that, then yes. It is personally identifiable information.

CHIEF JUDGE HOWARD: But what if you don't know that they have that ability, and you have no reason to know that? And maybe they don't have the ability, so they go out and obtain it after, once they get this data from you, totally off the hook.

ABBY THORNHILL: So I have a couple of responses to your question. First, the statute does limit this to knowing disclosure is a personally identifiable information. So if a company actually did not know, or perhaps the third party recipient of the data was misleading about what they would do with the information, there would be no liability.

CHIEF JUDGE HOWARD: It seems to me that if that's what the statute means, then it is a free for all. There can't be a limiting principle. If there is one, I'd like you to help me find it. And if your position is that there should be no limiting principle-- that, in fact, what Congress really intends by the plain language of this statute is that none of this information should be sold-- then I'd like to hear it.

ABBY THORNHILL: So I do want to make clear that we don't suggest that this isn't a broad statute. And it does cover a lot of information and a lot of disclosures. And given the context in the market for this information today, that's true. But I think what we might think of as a limiting principle here is that if any company, including Justice Connect, is worried about liability, they do have the option of simply asking their consumers for consent. So under b2d, written consent is a way to completely avoid any liability under this statute.

Further, if it's true that consumers actually prefer targeted advertising and this is something they want, it should be no problem actually to get that consent. But I have a feeling that people also don't understand at what cost they're getting those targeted advertisements. And that goes back to Congress's purpose in actually passing this statute. So the VPPA was in addition to a long line of legislation meant to continue to protect personal information found in records. And in the legislative history, we get from many senators different broad concerns about the ability of technology to amass data about individuals and actually specifically identify them.

For example, Senator Leahy who was one of the sponsors of the bill specifically suggested that soon it would be relatively easy for anyone to create a whole profile of a person, including who they call on the telephone, what they buy in a store-- that sort of information. Congress further even predicted that companies might start using this information for commercial interests. So they might actually do something like we see today with the Chloe Company and target advertisements based on the information and that profile that we can build about individuals.

And they increasingly thought that this would be a problem with time. So Senator Simon, for example, specifically said as we continue to move ahead, we must protect time honored values that are so central to this society. And that's what the VPPA was meant to do. And that's why the *Yershov* standard is--

CHIEF JUDGE HOWARD: Why should we care about all this legislative history coming from individual senators?

ABBY THORNHILL: Well some of the statements are from specific sponsors of the bill. But even if your honor is not persuaded by the legislative history, we're merely bringing it in to, again, reinforce what the text tells us alone.

CHIEF JUDGE HOWARD: So we can ignore it.

ABBY THORNHILL: We could ignore it if you would like, your honor. Because the text itself is broad, as we suggested earlier. It is all information that is capable of identifying individuals. And as the First Circuit noted in *Yershov,* had Congress intended such a narrow and simple construction--

CHIEF JUDGE HOWARD: So when you resort to your version of legislative history, are you saying that you are adding something? You are emphasizing something in the statute, or you're simply saying that it's completely consistent with the plain meaning of the statute? I'm not quite sure what you're saying.

ABBY THORNHILL: Yes, your honor.

CHIEF JUDGE HOWARD: Why you're quoting from the senators.

ABBY THORNHILL: So we're quoting from the senators just to clarify and to, as you suggest, just reinforce what is already told to us by the text. I think the First Circuit's description of the text, saying--

CHIEF JUDGE HOWARD: You're not getting, are you, to the point? Or are you? That this being remedial legislation, it's to be read broadly. And we can tell how broadly by listening to what they said at the time.

ABBY THORNHILL: I don't think we need the senators' statements at the time, specifically because the text of the statute is broad. And that's what the First Circuit suggested in *Yershov.* If they had intended a

narrow construction to include only identity information, they would have written the text in that way. Similarly, we can look to other definitions in the statute, for example videotape service provider. If they were only worried about the context of something like a Blockbuster revealing someone's video rental history, they could have defined a videotape service provider as a brick and mortar video store. Instead, they described it as any person or company that deals in similar audio visual materials. Similarly with personally identifiable information, they left the text broad.

And I want to clarify here that we're not saying that the meaning of the statute has at all changed over time. We're merely asking this court to continue to apply the statute to new examples of technology.

JUDGE OLDHAM: Is the information here that was sold to the Chloe Company the same as the information in *Yershov?*

ABBY THORNHILL: So in *Yershov* specifically, just to make sure I get this right, we did have the GPS location as well as unique device identifiers which were included in our bundle. So it is, yes, actually very closely similar to the information in *Yershov.*

JUDGE OLDHAM: And does it matter about the capabilities of the person to whom it's sold, or in this case the Chloe Company-- the company to whom it's sold?

ABBY THORNHILL: Yes. Yes, your honor. That is the operative question. So what are the capabilities of the third party, and did the videotape service provider-- were they aware of those capabilities when they gave the third party that information?

JUDGE OLDHAM: And I noticed in the district court's resolution of summary judgment in your favor, the district court doesn't say anything about the undisputed nature of the Chloe Company's capabilities. What do we do with that?

ABBY THORNHILL: Yes, your honor. So unfortunately, the district court opinion is not specific about its assumption. However in adopting the *Yershov* standard and then finding liability, we can assume that the district court did accept that. But further, I think your honor's question points us to something that is important. And that is the context in which this information is sold today. So it is sold to companies like the Chloe Company, where it is their explicit business model to take the information that they've gathered from different videotape service providers and other companies, aggregate it, and specifically identify individuals. In two of the circuit

courts that have addressed this issue, as well as one of the district courts, all the information was sold to Adobe. There's only a few actors in this space who are actually taking the information, and we know exactly what they're going to do with it.

JUDGE OLDHAM: Well, they know that they can identify an individual by a number, but they don't know that it's me as opposed to you. Right? They just know it's somebody. They know it's client 123456789. Right? So why does that fit within the text that you had urged earlier that we adopt so closely about personally identifiable?

ABBY THORNHILL: Respectfully, I'm not sure that you're correct that it is just an identifier. I think it is actually the entire profile of the person, because they're aggregating that with information they already have, which can include something like a name and address and actually pinpoint a specific individual.

JUDGE OLDHAM: Do we know that the Chloe Company has the names associated with the various otherwise anonymized data?

ABBY THORNHILL: Again unfortunately, the factual record doesn't specifically suggest that. However, if the district court did find under the *Yershov* standard that Justice Connect violated the statute, then we can assume that the Chloe Company was able to actually identify specific individuals.

JUDGE OLDHAM: Got it. So your position is absolutely that you'd need to be able to tie it to an identifiable person, not just an identifiable number.

ABBY THORNHILL: Yes, your honor.

JUDGE OLDHAM: Very good.

ABBY THORNHILL: But I know that my time is starting to run short, so I do want to get to what I sort of addressed as my third point in my introduction. And that is that this broad standard would be consistent with other uses of the phrase "personally identifiable information" throughout the government's statutes and regulation in this area. And I think this is important first, because two different videotapes service providers like Justice Connect-- this shouldn't be a surprise. This is the standard that is used throughout the privacy sphere.

But also in *Smith vs. City of Jackson,* the Supreme Court specifically held that when we have similar statutes with similar purposes, we can infer that Congress meant to give the terms in

those--

CHIEF JUDGE HOWARD: Don't those other statutes that you cite in your brief have more precise, less awkward language to use Judge Kayatta's descriptor? Or am I wrong about that?

ABBY THORNHILL: You're correct, your honor. In some circumstances, they did fully delegate authority to a regulatory agency to actually make the definition. But I that is important, in the sense that they are then leaving to the regulatory agency the actual fact finding and actual decision about what qualifies as personally identifiable information. With the VPPA, we simply have a different--

CHIEF JUDGE HOWARD: And Congress could certainly do that here, right?

ABBY THORNHILL: They could, but they left--

CHIEF JUDGE HOWARD: So you're suggesting that a common law approach would be better?

ABBY THORNHILL: No, your honor. I'm merely suggesting that in this context, they left the fact finding to the courts. And so they left the courts with the ability to actually determine what is personally identifiable information. And the text of the statute does not specify specific information, leaving it open for the courts to determine whether in a specific context, information is personally identifiable information.

Further, we can look to those statutes as well as regulations and statements from different regulatory agencies to determine what personally identifiable information means. So for example, the General Services Administration stated that information can be used to distinguish or trace an individual's identity, either alone or in combination with other information that is linked or linkable to a specific individual. Again, reinforcing this point that something on its face might not be identity information, may not readily show to someone who someone is and what they've done with their video rental history. For example, in the VPPA context-- but is more broad and can be used in aggregate.

CHIEF JUDGE HOWARD: Well the Federal Trade Commission, for example, has authority like this under one of its statutes, I take it. But it's an agency that is supposed to be protecting consumers. Congress chose not to take that step here. Why shouldn't we draw the presumption the other direction,

that it meant a more limited application here?

ABBY THORNHILL: Again, I would go back to the text of the statute. Congress specifically left it broad and open ended. It left it as all information.

CHIEF JUDGE HOWARD: Then how much help, really, is all this other stuff about what the executive branch agencies have the power to do under other statutes? How much help does it give your argument?

ABBY THORNHILL: It gives some help in the sense that we can look to similar statutes with similar purposes, often to infer intent. But if we only want to rely on the text, we can. Those further statutes do put Justice Connect and other actors on notice of what might qualify as personally identifiable information, but they certainly are not the only things we need here to decide this case. If there are no further questions, we ask this court to affirm the decision of the district court.

CHIEF JUDGE HOWARD: Thank you.

ABBY THORNHILL: Thank you.

CHIEF JUDGE HOWARD: Is there any rebuttal? Will you both be presenting, or just one of you?

MEGAN MERZ: May it please the court. Your honors, first I will address the issue of standing. And then, I will move on to my own issue on the Video Privacy Protection Act. So first on the issue of standing, I want to first start by noting that the standard here is not one of increased risk or plausible risk. The standard here is one of substantial risk. And the only definition that we have of substantial risk, which is a very vague term, is another far less vague term, certainly impending.

Now our friends on the other side cite to *Susan B Anthony List. Susan B Anthony List* does state that a harm can be certainly impending or a substantial risk, but it never clarifies a difference between those standards. The only clarification we have about the meaning of those standards comes from *Clapper* footnote 5, which treated them as the same thing. So for the purposes of this argument, the only more defining information we have about what substantial risk means is that it means a clearly, certainly impending type of risk.

So this standard under *Clapper* does not fit with what the plaintiffs have alleged today. This

would make this circuit the first of the eight that have considered this issue to find standing where no known misuse has already taken place in a data breach.

JUDGE NATHAN: But that's an argument that there has to be harm. And that's different than risk.

MEGAN MERZ: Well your honor, I don't think it's an argument that every plaintiff-- a plaintiff can come to the court and get standing, even if harm has not befallen them. But there has to be some evidence, some shrinkage of the attenuation chain to prove that there is actual misuse looming on the horizon for that particular plaintiff. We do think if in this case there was more evidence to debate, perhaps there would be a stronger case. But here, there is simply no allegation of a single dollar spent by plaintiffs in preventative measures. There is no allegation of a single attempted misuse. And that would set this court apart from all the other circuits that have considered this issue, including all the cases they cite, which all have found instances of misuse before finding standing for data breach plaintiffs.

This attenuation chain is also not just about intent. It's also about the ability of the hackers and the hinging on the fact that these people haven't just called and canceled their credit cards in this nine months that have passed since. But to move on to the VPPA issue. Both of these standards do treat differently with time how data is treated under this particular statute. I showed you how the ordinary person standard fits with the legislative history and that it evolves with time. But it doesn't evolve too much with time. We agree this is a broad statute, but it's not as broad as appellees suggest.

Can look to the quote that I read about reasonable, legitimate, enforceable extent of the privacy Congress intended to protect here. This wasn't intended to be protect the most consumer privacy possible. This was aimed at a specific swath of information. And Congress assumed there was other information these companies would be able to disclose that would not fall under this statute. But appellees have essentially written that information off, ignored that part of the statute's text, which implies there's other types of information. So while the statute focuses on the information itself, they focus on the recipient. So for these reasons, Justice Connect requests that you reverse both of the district court's orders. Thank you.

CHIEF JUDGE HOWARD: Thank you. Thank you all. We will take the case under advisement.

MARSHAL: All rise.

CHIEF JUDGE HOWARD: Court is still in session. You may be seated. Judge Oldham.

JUDGE OLDHAM: Well I have to say, I have obviously the least oral argument experience of anyone on our panel. But I have seen a lot of arguments in a lot of circumstances. A lot, I've been involved in personally, whether as an advocate or as a judge. And I cannot tell you how it almost makes me emotional how extraordinary all four of you are. I would take all four of you. It makes me proud of all four of you.

It makes me proud of my adopted Alma mater. I was saying earlier this afternoon how sad I am that I had the good judgment to come here undergrad and the terrible judgment not to come back for law school. You should be very, very proud of your university, very proud of the moot court competition, extraordinarily proud of all of the effort that you put into this.

It's a breathtaking sight to behold on the briefs. And in particular here today, all four of you were just extraordinary in your composure, your demeanor, your ability to answer difficult questions, your ability to pivot off of things that were challenging positions for your client, or the problem packet that the moot court board gave you and come back to positions of strength. And it gives me an incredible amount of confidence in our profession and the ability to have appellate litigators going forward. You should all be just incredibly proud.

One of the things that I loved about our conference-- we were talking about it as we were walking over here-- is how short and easy it was, given how just extraordinary all four of you are. And the one thing I think we could all agree on is that the shortcomings, the things that we were pointing out is little half point things here and there were little, itty bitty, teeny, teeny, tiny things. It was like separating the A plus plus from the A plus. It was really an amazing sight. So thank you, all four.

JUDGE NATHAN: I join in full. It is an absolute pleasure. I'll start with the briefs. I'm always blown away, at these kinds of things, by the oral advocacy. I'm not always blown away by the briefs. Both briefs were fantastic. There was never a moment of, what are they talking about, or sort of getting stopped by the language. The structure was beautiful. Your reliance on law was beautiful. Your creativity of argument was just superbly well done all around. And that's lawyering. Standing on your feet is lawyering, but 98% of the job of lawyering is the written work. And you all did fantastically with that.

As for the oral advocacy, as I said, I join Judge Oldham entirely. At base, oral argument is a

conversation. And it's not always the case, when we're actually in court, that we feel like we're engaged in a conversation with the lawyers, that they're helping us. They're really hearing the questions, and responding to the questions, and seeing what's troubling us, and helping us find our way. And all four of you did that fantastically. So I have nothing but compliments. It really was minor distinctions.

And it's hard with the scoring, because maybe someone seemed a little bit nervous or spoke a little bit fast. At the same time, that person might have had incredible control over the case law. And you know, in my book, probably control over the case law is what really matters at the end of the day. But you're influenced by some of these smaller things. It was really minor points of distinction, as my colleague said.

So my compliments to everyone. Also just to say, I think the trick to oral argument is anticipating the hardest questions that your side will face. And clearly, all of you had done that. And I tried to sometimes throw out things. I usually focus on procedure and throw that out. Did that a little bit today, but you all handled it well and actually gave me-- I thought oh, I'll really get them on this process question. But I didn't get a one of you. That was really well done. And my compliments to the writers of the problem, as well. That's not an easy task, and it came together very nicely.

CHIEF JUDGE HOWARD: So let me just add a couple of things on the briefs. It'll sound like an echo chamber. So I'm preparing for arguments next week. I have 18 cases coming up. I set them aside about 3/4 of the way through and picked up the briefs here. Now, I won't tell you which brief I read first. But what a treat it was! I mean, I set it down. I said why can't they all do it that way? I mean, it was just terrific. And then, I picked up the other side and said, uh oh. I don't know who wins on the merits. So really, kudos to both teams on the briefs.

And then, I just want to make another couple of comments on the advocacy today. It is absolutely true that all four of you came across, at least to me, like you were trying to help us. And that's what I'm looking for in every argument. I'm looking for that conversational tone. We know where the weak points are. We're not just here trying to win a case. We're trying to figure out where the law should be. And of course, it should be where our side says it should be. But I can't tell you what a rare skill that is. And when I see it, I know it. And I saw it in four advocates today. And again, I was very, very impressed.

Forgive me for being familiar, but I forget the last name. Henry, we threw some real curve

balls at you. And you recovered very well. You're never going to be in trouble like that again. So you're all set. Good job. And Katherine, I made a specific note that I think it was Judge Nathan or maybe both of us tried to throw you off. And what I was trying to do was to get you out of your argument quickly and see how wooden you were and mechanical you were in coming back. And I thought you came back very early on in your argument, really smoothly. I was quite impressed.

Megan, we tried to get you off your main point. And we tried and tried and tried. And you had to stick to that point. And you did it beautifully. I was very impressed by that. Am I doing it right, Abigail? Have I got them? Oh, good. Wait until I announce the results. Remember that Oscar's when they--

[LAUGHTER]

JUDGE OLDHAM: I'll do this.

CHIEF JUDGE HOWARD: You got it?

JUDGE OLDHAM: I got it.

CHIEF JUDGE HOWARD: Phew! OK. I noted a lot of things about all of you. But the one thing I just wanted to mention was that you had a lot of points that you needed to make in your favor. And any one of them could have stuck. But I really think the sum total was what mattered. And you got them all out, and you had impeccable timing. So good job, all. So thank you for letting me off the hook here.

JUDGE OLDHAM: Yes, I got you. I got you.

JUDGE NATHAN: You know, he's saying he's just going to correct you if you get it wrong.

JUDGE OLDHAM: No, you have to do it. I'm not getting you out of that. You still have to.

CHIEF JUDGE HOWARD: All right. Let me try this. So we did our individual scoring, but the board actually has this rubric that it follows. It includes the brief, and the oral, and you know, all this stuff combined. And what we were told is that it was razor, razor thin, and that the appellants team prevailed. And best oralist goes to Abigail Thornhill.

[APPLAUSE]

That was for you, and it was well deserved.