

UNITED STATES PATENT AND TRADEMARK OFFICE

---

BEFORE THE PATENT TRIAL AND APPEAL BOARD

---

ADOBE INC.,  
Petitioner,

v.

JONATHAN E. JAFFE,  
Patent Owner

---

IPR2024-01352  
Patent 6,757,828 B1

---

Record of Oral Hearing  
Held: December 9, 2025

---

Before JUSTIN T. ARBES, STEVEN M. AMUNDSON, and BACH V.  
HOANG, *Administrative Patent Judges*.

APPEARANCES:

ON BEHALF OF THE PETITIONER:

JAMES L. DAY, ESQ.  
WINSTON LIAW, ESQ.  
Farella Braun & Martel LLP  
One Bush Street, Suite 900  
San Francisco, CA 94104  
(415) 954-4414  
jday@fbm.com  
wliaw@fbm.com

ON BEHALF OF THE PATENT OWNER:

BRYAN D. ATKINSON, ESQ.  
Price Lobel Tye LLP  
500 West 5th Street, Suite 1205  
Austin, TX 78701  
(617) 456-8000  
batkinson@princelobel.com

The above-entitled matter came on for hearing on December 9,  
2025, commencing at 10:00 a.m.

P R O C E E D I N G S

- - - - -

JUDGE HOANG: Okay. Good morning. We're convened for oral arguments in IPR2024-01352, which pertains to patentability challenges of claims in U.S. Patent Number 6,757,828. I'm Judge Hoang. And I'm joined by Judge Arbes in the hearing room, and we have Judge Amundson appearing remotely.

So let's get started by -- with appearances for both parties who will be arguing today. If anyone else is attending in person or remotely with you today but not speaking, please identify them as well. So for example, please state if your client is attending. Following the hearing, please confer with the court reporter to ensure that there are no questions regarding the spelling of names in the appearance. We'll start with appearances for Petitioner.

MR. DAY: Good morning, Your Honors. James Day, on behalf of Adobe. I understand that my partner, Winston Liaw is listening in, and Tom Carmack of Adobe is also listening in remotely.

JUDGE HOANG: Thank you. And Patent Owner?

MR. ATKINSON: Good evening, Your Honors. This is Bryan Atkinson for Patent Owner Jonathan Jaffe. And I'm the only one attending for Patent Owner.

JUDGE HOANG: Excellent. Thank you. So a couple of notes before we begin. First, the court reporter will provide a transcript of the hearing that will become part of the record in the proceeding at a later date. To ensure the transcript of the hearing is clear, please speak directly into the microphone when talking and identify specific slide numbers, numbering,

1 and figures and any other pertinent information when referring to your  
2 demonstratives.

3 Second, for the hearing order, each party has 60 minutes total time  
4 to argue their cases. Petitioner will open the argument and may reserve  
5 rebuttal time. Patent Owner will then respond and may reserve surrebuttal  
6 time. Then Petitioner will present its rebuttal, followed by Patent Owner's  
7 surrebuttal. On objections, please remember that your argument should be  
8 limited to only those arguments previously presented in your briefs.

9 Please make it clear which claims you're addressing at all times.  
10 And we ask that the party hold any objections regarding your arguments  
11 until it is time -- until it is your time at the podium to note any objections.

12 Fourth, I'll maintain a clock and I'll try to give each party a five-  
13 minute warning during the opening argument and a warning near the end of  
14 any reserved rebuttal time. Our hearing room has a timer that I'll set up for  
15 each party with the requested time allotment but please keep track of your  
16 own time as well.

17 So Petitioner, do you wish to reserve any rebuttal time?

18 MR. DAY: Yes, Your Honor. I'd like to reserve 10 minutes.

19 JUDGE HOANG: Ten minutes? Great. Okay. Fifty minutes on  
20 the clock and you may begin your arguments when you're ready.

21 MR. DAY: Well, good morning, Your Honors. Again, my name  
22 is James Day. I'm here on behalf of the Petitioner Adobe. And of course  
23 we're here to talk about the '828 Patent owned by Mr. Jaffe. The '828 Patent  
24 claims a method of authenticating a data stream. And it's presented in the  
25 specification describes digital camera, a very high-level digital camera that  
26 can take an image at the same time it creates a signature. Then you can save

1 or send that image and signature to someone else.

2 At some later time, you can recalculate a second signature based  
3 upon on the image. And if the two signatures match, you know that  
4 validates that the image has not changed. If the signatures are different, then  
5 the -- something has changed and the image, it is not authentic. That's a  
6 high level of what's going on.

7 Just to sort of set the table for today's discussion, we have a  
8 number of different grounds of obviousness. For today's discussion, we're  
9 focused on prior art references, Glass, which we think alone renders the  
10 claims obvious; Rieger, which again we think alone renders the claims  
11 obvious; and then Serret-Avila, which can be combined either with Glass or  
12 with Rieger.

13 In any case, we think each of these grounds invalidate, render  
14 obvious all six of the claims. But for today's discussion, all of the disputes  
15 relate to Independent Claim 1. There are no separate disputes with regard to  
16 the dependent claims.

17 All right. Before we get to the claims, I do want to touch on the  
18 definition of a person of ordinary skill in the art, burden of proof. As we  
19 mentioned in our reply brief, parties largely agree on the definition of a  
20 person of ordinary skill in the art. The point of dispute is we believe our  
21 expert opined that such a person would have experience involving image  
22 processing.

23 Patent Owner disagrees. As we said in our reply, our expert, Dr.  
24 Xiong -- and I'm looking at Slide 6, which has his name on it, Dr. Xiong  
25 provides his legal framework. He cites evidence in support of his definition.  
26 Patent Owner, on the other hand, relies on Mr. Davis who doesn't say what

1 legal framework, if any. He applied, doesn't cite any evidence. He just  
2 asserts conclusory his definition.

3 One thing I want to point out here, Your Honors, when Patent  
4 Owner in the sur-reply is talking about the definition of a person of ordinary  
5 skill in the art, Patent Owner says, well, look, the point of the '828 Patent is  
6 just computer security, it's digital security and authentication, digital security  
7 rather than image processing.

8 And I'm looking at Slide 7, on the left-hand side, we've got Patent  
9 Owner talking about the '828 Patent in one context. But then on the right-  
10 hand side of the slide at a different point in the sur-reply, when Patent  
11 Owner is talking about the prior art, now, suddenly, the '828 Patent, like  
12 Glass and Rieger, is in the field of digital image security, its digital image  
13 validation that the '828 Patent is related to.

14 And there are particular problems inherent in digital image  
15 validation that are addressed by the patent, not by this Serret-Avila prior art  
16 according to Patent Owner. Again, same point, Serret-Avila is not  
17 concerned with the authentication of digital images according to the Patent  
18 Owner in a different part of the sur-reply.

19 JUDGE AMUNDSON: This is Judge Amundson. I have a  
20 question on the description of an ordinarily skilled artisan. And what I don't  
21 understand is why it's important that that person, that hypothetical person,  
22 have familiarity with image processing when the patent, in column 1, defines  
23 recordings broadly, to include audio recordings. Could you comment on  
24 that?

25 MR. DAY: Yeah. I think that the question here is a person of  
26 ordinary skill in the art is someone who will understand and be able to

1 implement the '828 Patent. Certainly, that person needs to understand how  
2 -- have some understanding of authenticating data streams generally. The  
3 claim talks about data streams. The point about image processing comes in  
4 because the '828 Patent describes the invention wholly in terms of image  
5 processing.

6 If you read through the patent, it's all about total image  
7 authentication. You take a picture and you authenticate it. There's a lot of  
8 discussions actually not related to the claims but about authenticating by row  
9 and column individual pixels. So the point is to understand the patent, you  
10 need some background in image processing. We think it's important  
11 because, as you get into this, the fact that Mr. Davis has no experience with  
12 cameras, digital cameras, digital images, we think it impacts the validity of  
13 his opinions, so that's why, Your Honor.

14 JUDGE AMUNDSON: All right. Thank you.

15 MR. DAY: And so on Slide 9, we sort of summarize where I think  
16 we are. Dr. Xiong exceeds the qualifications under our definition. Dr.  
17 Xiong meets Patent Owner's definition. There's some hint in Patent Owner's  
18 sur-reply that perhaps Dr. Xiong does not meet Patent Owner's definition.  
19 That would be a new argument. It wasn't made -- it's not clear that that's the  
20 argument in the sur-reply. It was certainly not made in response, so it would  
21 be forfeited. It's also incorrect.

22 I would point you all -- I'm looking at Slide 9. I would point you  
23 to Exhibit 1003, paragraph 5, that's Dr. Xiong's original declaration. And  
24 Exhibit 1029, paragraph 11, that's his reply declaration where he explains  
25 that he has experience that would meet Patent Owner's definition.

26 JUDGE HOANG: Counsel --

1 MR. DAY: Yeah.

2 JUDGE HOANG: -- do any of your arguments or Patent Owner's  
3 arguments turn on the definition or adopting one definition or another?

4 MR. DAY: Well, I don't think the arguments turn on it, Your  
5 Honor. But it goes, at least, to the weight of the evidence presented by the  
6 Patent Owner. Their expert is not -- we would say not qualified to offer the  
7 opinions he's offering here.

8 And I'll move to the next point, which I think makes the problem  
9 even worse. Patent Owner's expert applied the wrong and an improperly  
10 stringent burden of proof when analyzing the prior art and when considering  
11 our arguments of obviousness. Now, the Patent Owner applied a clear and  
12 convincing standard to invalidity, to obviousness. And of course, that's the  
13 incorrect standard. It's overly stringent. And so again, it's hard for me to see  
14 how you could rely on the evidence presented through Mr. Davis.

15 JUDGE ARBES: Counsel, the burden of proof is ours to apply to  
16 Petitioner and the experts opine as to whether they believe a reference  
17 discloses a particular limitation, for instance. But what is the relevance of  
18 this admitted mistake in the declaration? What are we to take from it?

19 MR. DAY: Yeah. Well, what I think the problem here is, Your  
20 Honor, when Mr. Davis is looking at the prior art and says, well, it doesn't  
21 disclose something, he's applying this incredibly stringent, very high  
22 standard of proof. So when you read what he says, well, it doesn't say lead  
23 or trace, and it could be anything. Therefore, there's a doubt in your mind  
24 about what's being disclosed. That's the wrong way to analyze prior art.

25 The way to look at the prior art is, is it more likely than not that it  
26 discloses what we say it discloses? That's the burden applied to us. That's

1 the way that an expert should view evidence. And it's not the way Mr. Davis  
2 views the evidence.

3 Okay. I'd like to move on to the disputes that involve the claim  
4 language. I have here on Slide 12 the claim language for Claim 1 on the left.  
5 And first, I want to talk about this limitation that refers to a sensor which is  
6 tightly coupled to the said memory.

7 And, really, the dispute centers on this phrase "tightly coupled."  
8 This "tightly coupled" is not a term of art. It's not defined in the patent. It is  
9 a term of degree. It's not just coupled; you have to be tightly coupled. And  
10 the Federal Circuit tells us -- we've cited here the Iridescent Networks case.  
11 We have other authority in our reply brief where you've got a term of  
12 degree, you've got to come up with some way to distinguish, you know,  
13 coupled from tightly coupled. And one way to do that is to look at the  
14 prosecution history.

15 You don't have to have some disclaimer. We can go back to  
16 Phillips. The prosecution history is always a relevant source of evidence  
17 when conducting claim construction.

18 And here, the prosecution history is the best evidence of what this  
19 term means. And what we point to in particular is during prosecution -- I'm  
20 now looking at Slide 12, during prosecution, the examiner rejected the  
21 claims over this prior art reference called Schipper.

22 And the Patent Owner changed all the -- actually, canceled all the  
23 claims, came up with all new ones. One of the limitations was this utilizing  
24 a sensor limitation. And they focus specifically on the tightly coupled  
25 language and said, well, you can see that in Figure 2A of the patent, it  
26 illustrates a processor which is tightly coupled to a memory.

1           And they say -- again, on Slide 13, I've highlighted -- because the  
2 processor is tightly coupled to the memory, it will be virtually impossible for  
3 a user to supply false information to the memory by breaking the conductive  
4 tracer lead between the memory and the processor. This language is  
5 important because this is the only example in the intrinsic record of a  
6 connection between two components that the applicants consider to be  
7 tightly coupled. This is our only example. And so we propose a  
8 construction that's consistent with that example, a sensor coupled to said  
9 memory via conductive traces or leads.

10           Now, this is the same construction that the District Court issued in  
11 a tentative order. That tentative order was -- the case was stayed before the  
12 judge issued a final order. But this does match the judge's tentative order in  
13 the District Court.

14           Okay. Now, let's talk about Glass. So in Glass, we've got Figure 3  
15 on Slide 15 in the upper right. And what's highlighted --

16           JUDGE AMUNDSON: This is Judge Amundson. I think I should  
17 have asked this a little earlier before you moved on. But could you just  
18 explain to us procedurally how we got a tentative order that's not signed by  
19 the judge and doesn't appear on the docket sheet?

20           MR. DAY: Well, what happened is we had a claim -- the judge  
21 issued a tentative order before the claim construction hearing. We then went  
22 to the hearing. The judge said, okay, I'll issue a final order. But he did not  
23 issue that final order before staying the case in light of this IPR. Frankly, I  
24 think the tentative order is in the docket in the District Court, and it is in the  
25 record before you, Your Honor. We submitted it as an exhibit.

26           JUDGE AMUNDSON: Right. Okay. Right. I saw it in -- I know

1 it's in the record of our proceeding.

2 MR. DAY: Yeah.

3 JUDGE AMUNDSON: Maybe I didn't look hard enough. But I  
4 didn't see it in the docket sheet of the District Court proceeding.

5 MR. DAY: Your Honor, I assumed it would have been -- if you  
6 didn't see it, I'm sure you're correct. He must have just sent it to the parties  
7 in advance of the hearing.

8 JUDGE AMUNDSON: All right. Fine. I just want to try to  
9 clarify that. Thank you.

10 MR. DAY: Fair enough.

11 JUDGE ARBES: Counsel, did the District Court judge say that he  
12 was adopting as the final -- that he would adopt as the final construction  
13 what was in the tentative order?

14 MR. DAY: No.

15 JUDGE ARBES: No?

16 MR. DAY: We had a hearing and he said he would issue a final  
17 order.

18 JUDGE ARBES: Do we have a transcript of the Markman hearing  
19 available?

20 MR. DAY: I don't believe it's in the record. There is a transcript  
21 of the hearing, and I'd be happy to provide it.

22 Okay. So Slide 15 is on the screen. We're talking about Glass,  
23 Figure 3. In the upper left corner of Figure 3, what's highlighted is a sensor.  
24 That's the optics, imager and digitizer. That's the sensor, frame store, 42.  
25 That's the memory. There's an arrow going from the sensor to the memory.

26 Glass states that solid line like that arrow is a data path. Glass

1 talks about sending the image from the imager and digitizer to store it in the  
2 frame store. Our expert opined that this digital image, that's how you send  
3 the data from one place to another inside this device and confirmed that a  
4 person of ordinary skill in the art would understand the data -- or the  
5 connection is by conductive leads or traces inside imaging system 4, you  
6 know.

7           How do we know that? Well, these are integrated circuits. Glass  
8 tells us the optics are perhaps a CCD camera, a CMOS device. The frame  
9 store is a memory. These are integrated circuits. And as our expert  
10 explained, because they're integrated circuits -- because they're inside of a  
11 device -- they're inside of a protected device, they're very close together.  
12 For all of these reasons, we know a person of ordinary skill in the art knows  
13 that they are connected by leads and traces.

14           And just to make sure we're all on the same page with regard to  
15 what leads and traces are, we created Slide 19. You can see there's a picture  
16 of an integrated circuit. The silver wires that come off the side, those are the  
17 leads. And now, if you look in the lower right corner, we have a picture  
18 taken from a prior patent figure.

19           And we've highlighted there on the right-hand side is the lead  
20 coming off an integrated circuit that is connected -- soldered to -- connected  
21 to a trace, which is a wire that runs through the board. This is how  
22 integrated circuits are connected together.

23           JUDGE HOANG: Counsel, did your expert rely on this exhibit in  
24 making his opinions?

25           MR. DAY: Yeah. These exhibits were cited in his reply  
26 declaration, Exhibit 1029.

1 JUDGE HOANG: Was there any other evidence that he used to  
2 support his testimony?

3 MR. DAY: In?

4 JUDGE HOANG: In his declaration, sorry. Were there any -- was  
5 there any additional evidence, such as this, that Dr. Xiong used to support  
6 his declaration?

7 MR. DAY: In the original declaration, he cited Glass, the  
8 prosecution history, and several parts of the prosecution history. He didn't  
9 cite these exhibits because these came in with our reply. I don't recall if he  
10 cited other evidence in that section, but there's a few pages where he talks  
11 about the leads and traces. Also, I would say, part of the discussion about  
12 leads and traces is also based just on an understanding of what Glass is  
13 disclosing.

14 And he has a summary of Glass which talks about the fact that  
15 these are -- you know, the sensor is a CCD camera integrated circuit. So in  
16 the original declaration, I think we also have to consider that summary of  
17 what Glass is disclosing and the fact that these integrated circuits are inside a  
18 single device, an imaging system that is inside of protective -- a secure  
19 packaging. That's important, too, because we've got integrated circuits very  
20 close to each other in a device, but they also want to be secure. And the way  
21 you do that is using leads and traces.

22 JUDGE ARBES: Counsel, there are a lot of arrows in Glass and  
23 Rieger. Is it your position that all of those arrows are conductive traces or  
24 leads? I believe Patent Owner pointed to an arrow in Rieger that was  
25 definitely not conductive traces.

26 MR. DAY: No. That's not our position at all, Your Honor. Our

1 position is -- I'm looking at Slide 18. The arrow from the sensor to the  
2 memory is by conducting leads and traces. It's from one integrated circuit to  
3 another. I'll move ahead to --

4 JUDGE ARBES: But those arrows do appear to be the same in  
5 Figure 3. There's a lot of arrows that appear the same.

6 MR. DAY: Yeah. I don't know the answer. I mean, our position  
7 is just that arrow. That's all that we're talking about. I confess I haven't  
8 even contemplated whether all of them have to be by leads and traces.  
9 That's not something that we've considered. And I would say, I saw the  
10 comment in the Patent Owner's slides. We're not saying every line in every  
11 figure must be leads and traces.

12 We're talking about that arrow that I've highlighted in Figure 3 that  
13 goes from the sensor to the memory. That's all we're talking about.

14 JUDGE AMUNDSON: This is Judge Amundson. On this point  
15 about conductive leads or traces, did you get to a point in the District Court  
16 litigation where Jaffe had to read that language on an accused product?  
17 Because I was wondering what they read it on, if they did.

18 MR. DAY: No. Your Honors, the infringement contentions in the  
19 District Court came before the claim construction. In those contentions,  
20 which were before this construction, they don't point to leads and traces.

21 JUDGE AMUNDSON: Oh, I see.

22 MR. DAY: It's not particularly helpful, I don't think. Okay. So if  
23 we're looking at Slide 20, this is our construction, and we think Glass meets  
24 it. Let me move to the next point, and that is Patent Owner -- so I'm on Slide  
25 21, and we have Patent Owner's proposed construction, a sensor that is  
26 electrically or physically coupled to memory in a device.

1           Now, I don't think that's correct. That seems to read the word  
2 "tightly" out of the claim. It's just two things that are coupled, electrically or  
3 physically, I'm not sure how else they could be coupled in this context. It's  
4 not based on, you know, a definition somewhere. And so we don't think this  
5 is the correct definition. But if you apply it, Glass -- and then I'll get to  
6 Rieger -- clearly meet it.

7           Glass has a sensor, the optics I've highlighted. Again, this is  
8 Figure 3. We know that the sensor, the optics, imager and digitizer, is  
9 sending data to the frame store inside a device, it's certainly electrically  
10 connected or electrically coupled, as Patent Owner's construction would  
11 require. So even under Patent Owner's construction, Glass meets it.

12           I'm going to quickly move to Rieger because the points are very  
13 similar. Rieger discloses a digital camera. There's a CCD sensor that's an  
14 integrated circuit. It's connected to a RISC processor, a CPU, that's an  
15 integrated circuit. They're both connected -- or the processor is connected to  
16 a RAM, that's an integrated circuit. The arrows show how the image data is  
17 sent from one integrated circuit to another.

18           These integrated circuits are inside a digital camera single device.  
19 Not only that, they're inside a protected section. So this is a secure area  
20 within a digital camera. And a person of ordinary skill in the art would  
21 know that the way you connect two integrated circuits together in this  
22 context, illustrated by Rieger, is via leads and traces.

23           And let me just -- to move things along, our expert establishes this  
24 both in his initial declaration and then there's further support in his reply  
25 declaration. But it's really -- it's the concept that you're using integrated  
26 circuits, they're inside a device and they're inside a secure part of that device.

1 So we think Rieger meets our definition.

2 Now, looking at Slide 26, again, Patent Owner's construction, we  
3 don't think is correct. But if you were to apply it, Rieger clearly discloses a  
4 sensor, the CCD sensor, that is at least electrically coupled to memory in a  
5 device. It easily fits within Patent Owner's construction.

6 Okay. Let me quickly touch on Patent Owner's response and the  
7 argument - the contrary argument, which is, well, there are lots of other  
8 ways you could send data from one place to another. And Patent Owner  
9 cites these three patents, Exhibits 2007, 8 and 9.

10 I'm looking now at Slide 28, saying, well, it could be -- you can  
11 use coaxial cable, you can use wireless, like Wi-Fi, you could use a satellite.  
12 There's a couple of problems here. First, it doesn't meet our evidence to say  
13 sort of, well, it could be leads and traces, but it could also be lots of other  
14 things. That doesn't meet the evidence we've presented. That sort of  
15 sidesteps the evidence.

16 We've shown that a person of ordinary skill in the art would  
17 understand that these connections are by leads and traces. And the Patent  
18 Owner's response is, well, it could be lots of things. So it doesn't meet the  
19 evidence we've presented. And even if it were true, it doesn't negate the  
20 evidence we've presented, which is that a person of ordinary skill in the art  
21 would understand these integrated circuits are connected by leads and traces.

22 The second problem is, you know, we asked our expert -- we  
23 actually asked two experts, Dr. Xiong and then Mr. Parulski. Mr. Parulski  
24 worked for Kodak for three decades designing digital cameras. We ask  
25 them, well, do you think a person with ordinary skill in the art -- looking at  
26 Glass' Figure 3, which is what's -- what matters, and that arrow between the

1 sensor and the memory? Or looking at Rieger's Figure 3 and those arrows  
2 between the sensor, the CPU, and the RAM, would a person of ordinary skill  
3 in the art think or understand that those connections are by a coaxial cable or  
4 by some wireless transmitter within the digital camera or up to a satellite and  
5 back down to go from the sensor to the memory half an inch away?

6 And both of our experts -- and these will be in Exhibits 1029 and  
7 1040, both of our experts said, no, of course not. And they explained why,  
8 space constraints, cost, security, lots of reasons why you would never  
9 -- probably would never even consider implementing Glass or Rieger in the  
10 manner that Patent Owner seems to be suggesting.

11 Okay. Before we move on, I did want to touch on some -- there's a  
12 footnote in the institution decision where you all invited the parties to  
13 comment on a passage from the file history. And I wanted to address that  
14 specifically in the institution decision, that's Paper 8, footnote 6.

15 And I'm looking at Slide 29 right now. You all noted that in the  
16 prosecution history, the applicant said, in accordance with the present  
17 invention, the claimed tight coupling requires that the connections between  
18 the sensor and memory not be physically accessible to a user. And the  
19 question was, how does this relate to the construction of claims?

20 So I wanted to answer that specifically. There's a couple of ways  
21 we cited this evidence. In our original petition, we cited it as evidence in  
22 support of our construction of the next step, the monitoring step. I'm  
23 looking at Slide 30 now. Because if you look at that step, monitoring the  
24 integrity of the tight coupling -- tight coupling is actually the words that are  
25 used at this point in the file history, so we cited in support of the meaning of  
26 that limitation.

1 But also, we, and our experts, cited this passage from the file  
2 history as support for why Glass and Rieger disclose a sensor which is  
3 tightly coupled to said memory because both Glass and Rieger easily meet  
4 this description of the invention. So whether you apply it to the utilizing  
5 step or the monitoring step or both, this evidence just further confirms that  
6 Glass and Rieger meet the claim language.

7 And then in our reply -- I'm still looking at Slide 30 -- we  
8 explained that, look, if you want to add to the definition of tightly coupled  
9 that the connection or the coupling is not physically accessible to a user,  
10 Glass and Rieger still meet it. I mean, we say so in our petition. Neither  
11 party is advocating for that construction. But if you were to adopt it, Glass  
12 and Rieger, both disclose it.

13 Okay. Let's talk about that next limitation, this is monitoring the  
14 integrity of the tight coupling. And what the patent talks about, it says -- this  
15 is -- I'm looking at Slide 32, during the operation of the camera, internal  
16 security is monitored to detect the integrity of the tight coupling between the  
17 sensor and the memory. And it says, several places -- here, you're running  
18 some checks on the camera. And one of them is a check 59 of the internal  
19 security system to see if there's a breach of security.

20 And if so you record it -- bottom of Slide 32, if internal security is  
21 compromised, security violation is appended to the image. These are the  
22 only discussions about internal security or monitoring integrity, anything.  
23 And what the patent is talking about is you monitor the internal security of  
24 the digital camera. And that is the way that you monitor the integrity of the  
25 connection by monitoring, you know, sort of the -- whether anybody has  
26 broken into the device.

1           It's not specific in the patent because it just refers to internal  
2 security. I think that's a reasonable way to construe what they're talking  
3 about. But I know that that's true because during prosecution, they  
4 confirmed so.

5           And here on Slide 33, what happened here is during prosecution,  
6 the examiner, again, rejected all the claims. And in response to that  
7 rejection, the applicants added the step of monitoring the integrity of the  
8 tight coupling, et cetera, through the end, that entire limitation was added.

9           And here on Slide 33, I show that the applicant said, well, look,  
10 Maloney -- the prior art reference doesn't have that. And then they say  
11 there's an exemplary disclosure in Figure 4A, which is a flowchart. And in  
12 the flowchart, there's this step 59, which is determining whether internal  
13 security has been compromised against this notion of internal security.

14           And then what they say is, what this limitation means is -- for  
15 example, a signal is generated if the device that protects physical access to  
16 the interconnections between the sensor set and memory is broken. A signal  
17 is generated if the device is broken. That's how you check internal security  
18 of this camera. Has somebody broken into the camera? That's what --

19           JUDGE ARBES: What, in your view, is "the device" referring to  
20 that's --

21           MR. DAY: It's a digital camera.

22           JUDGE ARBES: And how do we know that?

23           MR. DAY: That's what the specification -- that's all the  
24 specification talks about.

25           JUDGE ARBES: Well, if we go back to the slide before this,  
26 where we're talking about the first excerpt that you have there from column

1 4, "internal security 14 is monitored to detect the integrity of the tight  
2 coupling of the sensor set and the recorder 6." So it's not internal security of  
3 the camera as a whole, but it is specifically monitoring this particular  
4 connection, right? That's what it's disclosing --

5 MR. DAY: That's not the way I read it. First, it begins by saying  
6 during operation of the camera, so we're definitely talking about a camera.

7 JUDGE ARBES: True.

8 MR. DAY: Okay. So we're talking about a camera, and it refers to  
9 insert -- internal security. I read that to say it's the internal security of the  
10 camera. Has someone gotten into the internal parts of this camera? You're  
11 reading it a different way, Judge. And so that's why perhaps it's ambiguous;  
12 it's not to me, but it might be. So then I think this passage from the  
13 prosecution history is very important because it's not ambiguous at all.

14 Here, the applicants told the examiner what this limitation means is  
15 a signal is generated if the device is broken and the device is the camera.  
16 That's what they're talking about. That's how they got past Maloney. And  
17 that's how they got the patent issued. So they should be held to this  
18 language that they relied on.

19 JUDGE ARBES: One more question regarding the excerpt on  
20 Slide 33. The sentence before that does use the words "exemplary" and "for  
21 example." And then in the sentence you're referring to, it again it says "for  
22 example."

23 MR. DAY: Yeah.

24 JUDGE ARBES: So why should we read this as limiting, given  
25 that language?

26 MR. DAY: Yeah. Well, our proposed construction is not identical

1 to this language. And so I don't know that -- we're asking you to necessarily  
2 limit the outer scope of the claim to this language. What I'm going to show  
3 you is this language is virtually identical, if not identical, to what we see in  
4 Glass and Rieger. And so the point is almost no matter how you construe  
5 the claim language, we know Glass and Rieger disclose this invention  
6 because this is the way that the inventors described it to the patent office. So  
7 it's less a claim construction issue and more an evidence issue.

8 This is a statement by the Patent Owner saying, this is my  
9 invention, for example, this qualifies -- at least qualifies, right? And so  
10 because the prior art is at least -- or matches this example, it must disclose  
11 the claim language.

12 JUDGE HOANG: Counsel, why is it the device that prevents  
13 physical access to the interconnections between the sensor and the memory  
14 -- why isn't that device some specific device between the sensor set and the  
15 memory, as opposed to, you know, what you're asserting as the camera's  
16 body?

17 MR. DAY: Because there's nothing in the patent talking about  
18 that. I showed you the entire discussion of internal security in one slide, and  
19 it just says monitor internal security. I mean, there's no discussion in the  
20 patent about the connection between the sensor and the memory. We have  
21 to look at the file history for that. And so there is no other device. The only  
22 device we're talking about is the camera.

23 JUDGE ARBES: Is there any discussion in the specification of the  
24 camera preventing access to the individual components in it?

25 MR. DAY: No. It's just that -- what they say is, this is an inside of  
26 a camera and you monitor internal security.

1 JUDGE ARBES: So for purposes of trying to figure out what the  
2 device is broken means in this portion of the prosecution history, there's  
3 nothing in the specification that would illuminate this.

4 MR. DAY: Well, I disagree.

5 JUDGE ARBES: Okay.

6 MR. DAY: The specification only talks about a camera. That's  
7 the only device that we're talking about. And so the device that is broken is  
8 the camera. The flowchart 4A is a flowchart explaining the steps performed  
9 by a digital camera. The step of determining whether internal security has  
10 been compromised, that's performed inside a digital camera. The only  
11 device is a digital camera.

12 And so we know what this means. Has someone broken into a  
13 digital camera? And this makes sense, right? Take a step back. What we're  
14 talking about is you've got a sensor and a memory, and we want to know  
15 whether someone has had access to that connection so that they could have  
16 monkeyed around with it. The way you know that is, has somebody broken  
17 in?

18 This makes sense. If someone's broken into the camera, you can't  
19 trust that they didn't do something inappropriate because they broke into the  
20 camera. So it makes perfect sense. Even if we sort of step back a little bit  
21 and think about it.

22 JUDGE ARBES: I guess that begs the question, Counsel, why  
23 recite this particular language? Monitoring the integrity of the tight coupling  
24 between two things. If we're just talking about monitoring the integrity of  
25 the camera as a whole, why have that specific language?

26 MR. DAY: Like, they could have said that. But the point of

1 monitoring the integrity of the whole device is that it's important to know  
2 whether someone had access to that connection between the sensor and the  
3 memory. Certainly, the claim is talking about that -- the integrity of that  
4 connection. Did somebody have access to it? Is it possible that they did  
5 something to it? Is it possible that they, you know, spoofed a signal between  
6 those two devices?

7           We know it's possible if they broke into the camera. That's the  
8 point of this. We're not suggesting that the tight coupling is not important,  
9 it's just the way the patent says to monitor the integrity of that coupling is to  
10 determine if somebody broke into the device. And that's the way -- I think  
11 that's the way to read this passage in the prosecution history. I actually don't  
12 think there's any support to consider in a different way that the device is  
13 some other device. There just isn't any other device.

14           Further, we did cite this passage that I talked about a few minutes  
15 ago where the Patent Owners, the applicants, told the examiner the claimed  
16 tight coupling requires that the connections between the sensor and the  
17 memory not be physically accessible to a user. That's also relevant. It talks  
18 about the tight coupling. We propose this construction determining whether  
19 physical access has been gained to the connection. That's how you monitor  
20 the integrity. Has somebody physically accessed it? I think that's directly  
21 supported by these passages in the file history.

22           But I think even more importantly, just as an evidentiary matter,  
23 we know that both Glass and Rieger put these, the sensor and the memory,  
24 inside a protected or tamper resistant packaging. And so both Glass and  
25 Rieger -- I'll start with Glass. Glass says this entire package, including the  
26 sensor and the memory, must be tamper resistant. So it's extremely difficult

1 to access the internal elements without detection or destruction.

2 And Glass actually uses similar language. It's essential to ensure  
3 the integrity of the acquired image and codes to be sure they have not been  
4 compromised. And the way you do that in Glass is the imaging system will  
5 be enclosed in a tamper resistant package -- this is Slide 37 -- which will be  
6 used to detect unwelcome intrusion and render the system useless.

7 So continuing, one more, Slide 38, Glass describes this Switch 51.  
8 It's an intrusion detector or switch 51 that sends a signal to the processor if  
9 somebody breaks in.

10 JUDGE AMUNDSON: This is Judge Amundson. On the  
11 -- interpreting the meaning of the monitoring the integrity of the tight  
12 coupling phrase, as I understand Adobe's position, you were proposing that  
13 the Board adopt the same construction that the District Court tentatively  
14 adopted. Do I have that right?

15 MR. DAY: Your Honor, that's correct. Although, I guess what I  
16 would say is the disclosure in Glass -- and Rieger, when I get to it -- is so  
17 consistent and is exactly the same is what the Patent Owner -- what the  
18 applicants told the patent office in order to get the patent issued. In this  
19 quote on Slide 39, that almost regardless of how you construe the claim  
20 language, we know that Glass and Rieger fit within it.

21 But back to your question, you're exactly correct. We propose a  
22 construction that is the same as the construction the District Court judge  
23 adopted in the tentative order. But again, I don't think the construction  
24 actually matters because Glass and Rieger are exactly the same as what the  
25 Patent Owner said to the examiner to get the patent issued.

26 JUDGE ARBES: Counsel --

1 JUDGE AMUNDSON: Go ahead.

2 JUDGE ARBES: Thanks. Counsel, Patent Owner -- back to claim  
3 construction. Patent Owner argued that the claim expressly requires  
4 monitoring of the tight coupling between the two components. How do you  
5 respond to that?

6 MR. DAY: Well, okay. Let me move ahead a bit. So I think  
7 what's happening there is the Patent Owner is actually rewriting the claim  
8 language a little bit. I'm looking at Slide 42. And we put a quote up from  
9 Patent Owner's response, which I think illustrates the problem with Patent  
10 Owner's proposal, which is to rewrite the claim to say that it -- to rewrite the  
11 claim to say monitoring the tight coupling between the memory and sensor  
12 specifically.

13 So the claim doesn't say monitor the tight coupling. It says  
14 monitor the integrity of the tight coupling. The integrity of the tight  
15 coupling means has someone had access to that tight coupling? It doesn't  
16 say monitor the tight coupling specifically. They could have written the  
17 claim that way. They could have said, you need this monitor on the tight  
18 coupling.

19 Now, I don't think it would have been supported by the patent  
20 specification, but they could have tried. Instead, they used different  
21 language, it's broader language. What the specification talks about is  
22 monitoring internal security, which is a broader concept than monitoring a  
23 wire, a particular wire. And they clarified -- we did clearly clarified in the  
24 file history what this language means when they said it's determining if  
25 somebody broke into the device.

26 Okay. Let me move ahead to a different issue if I may. And this is

1 the limitations that have to do with generating an "ok" or an "error" signal.  
2 And I'm looking at Slide 44. In the claim language -- now, we've been  
3 talking about the part of the claim where you're capturing an image, where  
4 you're collecting the data stream and you generate a signature. Now, we're  
5 going to talk about the part of the claim where at some later point you can  
6 authenticate that image. So has something changed or not?

7 And if you look at the claim actually on Slide 44, just above the  
8 highlighted part, it says what you do is you generate a second signature and  
9 then you compare the step -- you perform the step of comparing said first  
10 signature to said second signature. And then there are two possible results.  
11 If the first and second signatures are not the same, then you give a signal that  
12 there's an error indicating that the image is not authentic. If the signatures  
13 are the same, then you generate an ok signal displayed to the user to indicate  
14 that the data stream, the image, is authentic.

15 Okay. And in Glass, we pointed to this image authentication  
16 module. This is Figure 8 of Glass, it's on Slide 44. That module performs  
17 the comparison that's described in the claim. There's no dispute about that.  
18 And then the image shows that -- the image authentication -- I'm sorry, the  
19 figure shows that the image authentication module determines whether the  
20 image is "ok" or "bad." And that information is put into a log file.

21 Glass tells us we prefer to log every step. We record the  
22 transaction because this data can provide irrefutable evidence of the  
23 transaction if it's required. And so we think that this meets the claim  
24 language.

25 Patent Owner responded to this by saying in Patent Owner's  
26 response, no, no, no, you have to display some error/ok message when you

1 authenticate the image, when it was all about doing it at the same time. We  
2 noted in our reply brief, no, no, no, the patent doesn't say that; there's no  
3 timing requirement. If you look at the log file the next day, that's sufficient.

4 And so in the Patent Owner's sur-reply, they pivoted and said, no,  
5 it's the mere possibility of display that's insufficient. The issue is not about  
6 temporality but rather certainty. We don't know for sure that someone's  
7 going to look at that log file every time.

8 Well, there's a couple of problems here. One is this a new  
9 argument, it should be forfeited. But even more importantly, it's legally  
10 incorrect. On Slide 46, we cite the Federal Circuit in the Unwired Planet  
11 case, noting that prior art that sometimes meets the claim elements is  
12 sufficient to show obviousness. Because we know the log file is going to be  
13 reviewed as irrefutable evidence if required, that means sometimes the error  
14 -- the ok or the bad, the error or ok signal is going to be displayed to the  
15 user, that discloses the limitations.

16 Patent Owner also --

17 JUDGE HOANG: Counsel, you have four minutes left.

18 MR. DAY: Yes, thank you. Patent Owner also made this  
19 argument that the user might not have access, maybe only a system  
20 administrator would. The log is going to be held on some server, might be  
21 somewhere else.

22 There's a couple of problems with this argument. One, again, it's a  
23 new argument. It wasn't in the Patent Owner's response, it's forfeited. But  
24 the fundamental problem is this defines the term "a user" in the claim  
25 language to exclude an administrator. And the plain meaning of "a user" is  
26 anyone using the system.

1           The person using the system at this point is someone who's trying  
2 to authenticate an image that could very well be someone using Glass'  
3 system to determine if someone else was trying to break into it. And so it  
4 could very well be an administrator. And so I think there's a problem with  
5 that analysis, even if you consider it.

6           I want to talk about Rieger for a minute. And the important thing  
7 with Rieger is -- we cited this Figure 7, it shows a very similar sort of  
8 analysis, this integrity test, so Rieger is talking about a digital camera. You  
9 take a picture, it gets signed. You can then save it or send it to someone else  
10 who can use a hash function to create a second signature, compare it to the  
11 first.

12           And what Rieger says is if the hashes match, you've authenticated.  
13 If they're different, you know that something has changed. And in the  
14 figure, we see a smiling face or a frowning face that's similar to the ok/bad  
15 in Glass, it's telling you the result.

16           Patent Owner seems to take this position that this doesn't disclose  
17 displaying to the user, I guess, thinking that the user might conduct this  
18 integrity test but not learn the result, which seems counterfactual and  
19 illogical. What Rieger is talking about is an integrity test where you receive  
20 this image, you receive the signature, and then it says a user can compare  
21 -- can calculate the second signature and compare it to the first.

22           And what Rieger says is the user can compute the hash value  
23 himself on the basis of the original plain text and determine -- the user is  
24 going to determine, learn, be informed, discover, be displayed the result of a  
25 comparison to determine whether the value transmitted by the sender is  
26 identical with their own result. The reason you conduct this integrity test is

1 to learn the result of the integrity test, and therefore it must be displayed to  
2 the user.

3 Rieger refers to a user. We know this has to be true. Rieger's  
4 talking about a camera to generate images that can be used later in court as  
5 evidence.

6 On Slide 50 -- I'm not going to go through this -- all of this. But  
7 Rieger's very clear. What he's trying to do is take pictures that later can be  
8 validated so you can use them in court or learn that they've been  
9 manipulated so you can't use them in court. It's nonsensical to think that you  
10 would conduct that test and not learn the result.

11 And finally, Serret-Avila, I don't have time to go through in great  
12 detail. But the point here is Serret-Avila says -- and what we're using is  
13 -- just looking at Figure -- Slide 54. Serret-Avila has a flowchart, it's Figure  
14 5 -- let me back up, Figure 5 on Slide 53 that really walks through this  
15 comparing and then the two "if" statements and the figure has the  
16 comparison, that's 514 in the figure where you compare the first and second  
17 signatures.

18 There's no dispute that that's what's happening there. And then if  
19 they're different, Serret-Avila says, you can take defensive action, including  
20 display a warning or an error that meets the claim language. If they're the  
21 same, then the block of data that you're analyzing can be released. What  
22 does it mean to release the data for use -- released for use? For example,  
23 you can display it on a screen, you can print it.

24 In either case, that content, the thing you just authenticated, is  
25 presented, displayed to the user. That's an indication that the content is  
26 authentic. So with Serret-Avila, either you're going to see an error message

1 or you're going to see the image. And if you see the image, you know it's  
2 been authenticated because it's one or the other. That's the way Serret-Avila  
3 works.

4 I'm going to -- why don't I stop there and reserve the rest of my  
5 time, please.

6 JUDGE HOANG: Thank you, Counsel. You'll have nine minutes  
7 of rebuttal time.

8 Okay. Patent Owner, do you wish to reserve any rebuttal time?  
9 You're muted, Counsel.

10 MR. DAY: Do I need to do anything to change over?

11 MR. ATKINSON: Yeah. I'd like to reserve seven minutes of  
12 rebuttal.

13 JUDGE HOANG: Okay. Seven minutes. Thank you. Let me set  
14 this clock up. Okay. You've got 53 minutes on the clock. Thank you.

15 MR. ATKINSON: Sorry. Let me -- Your Honors -- or good  
16 morning, Your Honors. So I believe that Counsel started with a discussion  
17 of the '828 Patent. But before I got into -- get into that, I'd like to discuss the  
18 issues that Petitioner briefly mentioned regarding Petitioner's expert and  
19 Patent Owner's expert and the relative expertise that the two experts had.

20 So Petitioner's expert, Dr. Xiong, is primarily a video and image  
21 coding expert. But he is not -- if you look at Dr. Xiong's CV, he has very  
22 little expertise in computer security, specifically. He has a great deal of  
23 expertise in video and image coding but not -- he's not particularly claimed  
24 work (PHONETIC) in the specific field of security. Whereas if you look at  
25 Mr. Davis' CV, you'll see that for, like, I believe the past nine years he's been  
26 a security researcher at Syscall.

1           So the two experts, they -- I don't think that either expert is  
2           unqualified to present, you know, their expert opinions, expert analysis on  
3           the patent and the reference that we're talking about here today. But I would  
4           say that to the extent that there is a question of expertise, the '828 Patent  
5           itself, it takes the image and video -- or takes image coding -- you know,  
6           kind of what comes out of the camera has a base, it's just kind of assumed.

7           And then it applies -- most of the work that's being done in the '828  
8           Patent involves ensuring that the added information that's used to encode the  
9           image that's coming from the camera has not been tampered with. And so,  
10          really, most of the work that's being done is more in the area of security  
11          rather than in the area of image coding. Because there really isn't -- you  
12          know, anything that's being done in the '828 Patent is not really focused on  
13          the specific area of image and video coding specifically.

14          As I mentioned and as Counsel discussed, '828 Patent, it  
15          authenticates digital files. And what it does is it uses a digital signature  
16          that's used -- that's created using the file as well as an outside parameter  
17          that's representative of at least one condition under which the digital sample  
18          was acquired. And some examples that are provided the '828 Patent are  
19          -- can be the date and time that the file is created, the compass heading, i.e.,  
20          what direction the camera's pointing when the image was taken. And also,  
21          potentially the altitude or, you know, the distance above sea level that the  
22          camera was at whenever the image was taken.

23          JUDGE HOANG: Counsel, may I just ask you to refer to your  
24          slide numbers, please?

25          MR. ATKINSON: Oh, I'm sorry, I'm up to Slide 5. And so we use  
26          this digital signature to authenticate the file using hashing algorithm. And

1 this also avoids the need for encryption. Because of that information, if  
2 there's any -- the way the hashing algorithm works is if there's any small  
3 change in the information that's used, then there is a -- there's a -- basically,  
4 there's a vast -- their -- the two results are completely different.

5 So the first issue that we have is the construction for the term, a  
6 sensor which is how they coupled to said memory that appears in Claim 1.  
7 Petitioner's proposed construction is a sensor coupled to set memory via  
8 conductive leads or traces. Patent Owner's proposed construction, the sensor  
9 that's electrically or physically coupled to memory in a device.

10 And I think that -- but the real issue is that when you look at the  
11 usage of the language conductive trace or lead from the prosecution history,  
12 when you look at how that's applied in the prosecution history, it's not saying  
13 that tightly coupled is limited to connections that are by conductive leads or  
14 traces only. It's saying that conductive traces or leads are examples of things  
15 that can result in a tight coupling. What makes the coupling a tight coupling  
16 is actually the monitoring of the connection, not necessarily -- oh, go ahead.

17 JUDGE AMUNDSON: This is Judge Amundson. I'm just trying  
18 to understand the scope of Patent Owner's proposed construction. And you  
19 say it's electrically or physically. What I'm trying to understand is if you  
20 could give us an example of a coupling that would only be physical and  
21 wouldn't have any electrical aspect to it.

22 MR. ATKINSON: So I think, electrically and physically are  
23 effectively the same thing in -- at least in the field that we're talking about  
24 here, which is electronic devices where you would have a -- you can't come  
25 up with connections that are not electrical and not physical, such as, you  
26 know, the easiest one is the Wi-Fi connection, also the satellite connection.

1 So both those are electrical and physical connections.

2 So I mean, maybe you could -- electrical and physical might be  
3 more accurate. But the emphasis is on those electrical and physical and not,  
4 you know, just by the specific example of a specific electrical and physical  
5 connection by conductive leads or traces.

6 JUDGE AMUNDSON: Okay. I think I got it.

7 JUDGE HOANG: Counsel, this is Judge Hoang.

8 MR. ATKINSON: Okay.

9 JUDGE HOANG: So let's assume we take your construction,  
10 electrical and physical. Then in that case, you know, you've been talking  
11 about Wi-Fi signals. Wouldn't they, Glass or Rieger, meet this limitation?

12 MR. ATKINSON: Well, we can get to that. The issue is that  
13 Glass and Rieger, both don't say what the connection specifically is. Now, I  
14 mean, it definitely could -- there's definitely the possibility that the  
15 connection is electrical or physical connection. But the -- neither really  
16 gives any information as to what connection is, you know, between the  
17 memory and the -- basically the sensor.

18 JUDGE HOANG: Counsel, is there any -- Counsel, do you know  
19 of any other way to send data from one component to another component in  
20 this type of electrical system? And do you have evidence of any other way  
21 that's not electrical or physical?

22 MR. ATKINSON: So as we point out in our response and in our  
23 sur-reply, both -- there are operative connections that are not electrical or  
24 physical, such as Wi-Fi connections or -- and -- as well as, you know,  
25 connections by satellite. Now, I mean within a single device, you know, it's  
26 definitely -- it would definitely be unusual to have a Wi-Fi connection, but it

1 is possible to have a wireless connection.

2 JUDGE HOANG: Are you saying a Wi-Fi signal is not an  
3 electrical or physical connection?

4 MR. ATKINSON: Right. That is what we're saying, that the Wi-  
5 Fi connection is -- it's a connection by waves. But there isn't a physical  
6 connection or electrical connection because it's just through the air.

7 JUDGE HOANG: Does your expert testify that electromagnetic  
8 waves are not an electrical or physical connection or phenomenon?

9 MR. ATKINSON: I don't think that we -- I don't think he testified  
10 specifically that electromagnetic waves are not. But he did testify that that  
11 Wi-Fi was an electrical connection.

12 JUDGE HOANG: Thank you.

13 MR. ATKINSON: And so as I say, whenever you look at the  
14 prosecution history, it repeatedly emphasizes that the exemplary nature of  
15 this example where the conductive leads or traces when -- you know, this is  
16 on Slide 8, conductive leads or traces, you see that third line from the bottom  
17 of the snippet on -- from the prosecution history?

18 But you see, surrounding it is exemplary structure, exemplary  
19 embodiment. And the emphasis is repeatedly that conductive leads or traces  
20 are just one type of electrophysical connection. But the emphasis on that  
21 connection that makes it virtually impossible for a user to supply false  
22 information, that's -- that I think is really the key is the -- tight coupling is  
23 one where it's impossible for a user to supply false information between the  
24 sensor and the memory.

25 JUDGE HOANG: Counsel, in that portion of the prosecution  
26 history that you've highlighted, all of the sentences describing exemplary

1 structures or exemplary embodiments, they're not -- they don't seem to be  
2 talking about the tight coupling. So for example, the sentence before the  
3 "because," it says it's discussing exemplary embodiments about generating  
4 random strings for authentication.

5 And then the next sentence, which does talk about tight coupling  
6 seems to imply, right, that the type coupling will have a conductive trace or  
7 lead. I don't see where in the prosecution history is specifically saying using  
8 a conductive trace or lead is an exemplary embodiment or structure.

9 MR. ATKINSON: So what it does is it says that the structure  
10 that's being described is exemplary structure for what tight coupling is. And  
11 then it goes on to describe what this exemplary structure -- you know, what  
12 embodiment is. And so in that embodiment, the structure is a conductive  
13 trace or lead. But that's only exemplary structure because it sets it up as that  
14 structure as being an exemplary structure in the prior two sentences, if that  
15 makes any sense.

16 JUDGE HOANG: Thank you.

17 MR. ATKINSON: So you see exemplary structure in the first  
18 sentence on Slide 8. And then you see exemplary embodiment in the second  
19 sentence, Slide 8. And then in the third sentence, it goes on to describe that  
20 exemplary structure is -- that exemplary embodiment -- and that exemplary  
21 structure, exemplary embodiment is by -- is one in which is conductive trace  
22 or lead. But those are -- that is consistently exemplary in setting up what is  
23 being talked about.

24 JUDGE HOANG: Understood. Thank you.

25 JUDGE AMUNDSON: This is Judge Amundson. I had a follow-  
26 up question on that. And wherein your excerpt from the prosecution history,

1 it states, it will be virtually impossible for a user to supply false information  
2 to the memory by breaking the conductive trace or lead between the memory  
3 and the processor.

4 And this is my question, maybe I'm being too literal here, but if  
5 someone -- to me, if someone broke the conductive trace or lead, that would  
6 be like damaging the printed circuit board. And maybe it should have said  
7 something like breaking into the conductive trace or lead. Am I  
8 misanalyzing this about breaking, like physically destroying the integrity of  
9 the leads, or what?

10 MR. ATKINSON: So I think what -- I think there may be a bit of  
11 difference. But I think what they meant was if you're able to gain access to  
12 the connection, i.e., if you're able to supply false information in between the  
13 sensor and the memory, that results in the breaking of the connection  
14 because you're able to provide false information.

15 And the assumption is that you're not able to provide that false  
16 information to the connection. You're not able to basically put an  
17 intermediary electrical connection in that provides, you know, false data  
18 because there's this internal security that protects that connection.

19 JUDGE AMUNDSON: All right. Thank you.

20 MR. ATKINSON: And so as we previously saw the Schipper  
21 reference, it was distinguished because it involved the external -- Schipper  
22 explicitly did use external information. And so that was the distinction  
23 between Schipper and the patent. Because Schipper used information  
24 explicitly originating from outside the camera. And so that's why you knew  
25 for sure in Schipper that you were getting external data. This is on Slide 9.

26 On Slide 10, the other claim construction we have is monitoring

1 the integrity of the tight coupling. And Petitioner's post-construction, it just  
2 relates on determining whether physical access has been gained to the  
3 coupling, whereas Patent Owner's proposed construction says determining  
4 whether physical coupling between the memory -- between said memory and  
5 said sensor has been accessed or disturbed.

6 And so we think Patent Owner's proposed construction is more  
7 accurate because consistently, we think that what the prosecution history and  
8 the patent talk of this internal security that specifically monitors and  
9 determines whether the connection, i.e., the data connection between the  
10 sensor and the memory has been accessed through the server, whether that  
11 connection itself is undisturbed.

12 And on Slide 11, we see the portion of specification that talks  
13 about the internal security, it says, during the operation of the camera,  
14 internal security 14 is monitored to detect the integrity of the tight coupling  
15 of the sensor set and the recorder 6, which is the sensor. So the specification  
16 is talking about the system checking this internal security system to make  
17 sure that a violation is not being recorded. And if the security has been  
18 compromised, then there is a security violation and that security violation be  
19 appended to the image. And so that's how -- yes?

20 JUDGE ARBES: I'm sorry, Counsel, can you give us an example  
21 of, or describe how the operation would work of detecting the integrity of  
22 the tight coupling between those two components, but not overall detecting  
23 the integrity of the camera as a whole? The Petitioner has drawn that  
24 distinction and believes that the language you're pointing to is more directed  
25 to the latter. Can you describe how it would work, in your view, to detect  
26 only the integrity of that tight coupling?

1           MR. ATKINSON: So I think what you could do is you could have  
2 a protective shield that -- like, on the circuit board that would overlay the  
3 sensor and the memory, and that would not be a very large area because  
4 these -- as Counsel mentioned, in the area of integrated circuits, typically  
5 you might have an integrated circuit that would be providing memory and  
6 you have another integrated circuit that would provide the CCD camera.  
7 And so it would be a very minimal amount of space between the CCD  
8 camera sensor and the memory that you have to house.

9           And you might have, like -- I mean, there -- it doesn't really go into  
10 any details about how you might do it, but you might have a small protective  
11 housing over those two components that would make sure that the  
12 connection between those components was undisturbed. What we know is  
13 that you're not -- is that the user isn't -- is that that connection itself is  
14 modern and that is accessible to the user.

15           JUDGE ARBES: Is there anything in the record before us that you  
16 would point to, to describe that example a bit? There -- you can see,  
17 obviously, there's no such language in the specification. So what else in the  
18 record would support your view on that?

19           MR. ATKINSON: Frankly, the specification record doesn't go  
20 into a great deal of physical details about how the connection between the  
21 camera and the memory is secured. It merely makes the point that that  
22 connection is secured.

23           And moving to Slide 12, we see from the prosecution history the  
24 description where it says that a signal is generated if the device that -- so,  
25 you know, like I say, all we know is that there's a device that prevents  
26 physical access to the interaction between sensor set and the memory. And

1 when the device that prevents that physical access to the interaction between  
2 sensory -- sensor set and memory is broken, that's when you get the  
3 violation. And so the answers here would have --

4 JUDGE ARBES: Counsel, just one question. Petitioner has taken  
5 the position that the words "the device" in that sentence are referring to the  
6 camera as a whole. Presumably, you disagree with that. What supports your  
7 view of that?

8 MR. ATKINSON: Because it says -- and it doesn't -- I think this is  
9 a new argument that we hadn't seen, frankly, before today. But when it says  
10 a signal is generated, it does -- when it says, "the device," it's talking about  
11 the -- I think it's talking about this -- the internal security device.

12 When it says, "the device," I think he's talking about internal  
13 security 14 and not the camera as a whole. So there's the internal security 14  
14 and -- the internal security 14 is what prevents physical access to the  
15 interconnections between the sensor set and the memory.

16 Because there -- it doesn't talk about -- you know, I mean, it  
17 doesn't say that there's no ability to access any part of the camera. In fact, I  
18 mean, that'd be kind of surprising just generally because you might -- you at  
19 least would need to, like, do stuff, like change batteries and stuff like that.  
20 And the devices -- I mean, what it -- there -- I just don't -- I don't see the  
21 entire camera itself as being -- what is the device? I mean, I think the device  
22 pretty clearly is what's being termed internal security 14. Or in this portion  
23 of the prosecution history, the 14 isn't there but internal security is there.

24 JUDGE ARBES: Counsel, what exactly is internal security 14? Is  
25 it a device? What is it?

26 MR. ATKINSON: Yeah. I think it is a device. But it doesn't

1 -- there's not any design details on what the device is. And apparently, it's  
2 known to a person of ordinary skill in the art. And it's just something that is  
3 used to prevent physical access to the interconnection itself.

4 JUDGE HOANG: And what evidence do you have that the  
5 internal security described in the patent would be specifically protecting the  
6 interconnections between the sensor and the memory?

7 MR. ATKINSON: It would be the description from the  
8 specification that cited on Slide 11 and -- as well as the -- as this piece of the  
9 prosecution history on page 293, shown on Slide 12. I mean, that's -- there  
10 aren't a lot of details given on what the internal security is. It's described  
11 operationally rather than physically.

12 JUDGE AMUNDSON: This is Judge Amundson. On that point,  
13 could you give us some examples of what that internal security could be,  
14 structural examples? I'm trying to get my arms around this. It's tough for  
15 me to envision it without some examples. So if you could do that, I think  
16 that would help.

17 MR. ATKINSON: Sure. So I think, you know, if you have a  
18 -- basically, a shielded piece that that sounds -- that set on a circuit above the  
19 CCD and basically engulf the CCD and the memory, which is -- like I say,  
20 on the circuit board, that'd be a short area. It is limited to specifically a  
21 circuit board.

22 But, you know, whatever it is, you just want to make sure that  
23 -- because the camera and the memory are -- would typically be -- I'll say  
24 camera -- when the camera sensor would typically be connected to a  
25 memory almost directly, there wouldn't be a lot of intermediary connection.

26 So whether it's by a cable or, you know, circuit board or whatever

1 the connection is, you would have the connection protected in a -- basically  
2 a shielded area. If you had a metallic shield that encompass both  
3 components, and then if the metallic shield was broken into or disturbed,  
4 then you would know that the -- someone had gained access to the  
5 connection between the camera and the memory.

6 JUDGE AMUNDSON: All right. That helps. Thank you.

7 MR. ATKINSON: Moving on to the two references. So we have  
8 -- the two main references I think we'll be discussing, they are the Glass  
9 references, U.S. Patent 6,332,193. And Glass, it collects biometric data  
10 from a sensor. And in one embodiment, that sensor is a camera too. I think  
11 it can get data such as like imaging or -- it's basically to potentially  
12 fingerprint a type of thing that's collected by the sensor.

13 And then it's using information to authenticate the -- that  
14 -- basically that fingerprint image and transmits those -- that information to a  
15 server. The server authenticates, they use the secret key and the transaction  
16 token, which is that -- base that extra information.

17 And so in Glass, the first issue we have is that we know that we  
18 have an optic -- we have this optics and camera 6. We have this digitizer  
19 and frame store 8. And we know that there's an operative connection  
20 illustrated by this arrow from the optics to the frame store. That's illustrated  
21 in Figure 2 of Glass. But we don't have any other details about what that  
22 connection is. We know that's operative -- we don't know whether it's -- we  
23 don't even know whether it's electric or physical.

24 We just know if there is an operative connection. We don't know  
25 what -- whether that is a connection that is physical or electrical. I mean,  
26 frankly, there's just not any description of how the -- these two components,

1     6 and 8, are connected within the Glass reference.

2             And we also see that a similar figure in Figure 3, we see that  
3     basically the same ones we see this -- the imager and digitizer attached,  
4     center image, to the frame store within this tamper resistant section. Again,  
5     we don't know how or what the connection is between the imager and the  
6     digitizer and the frame store. We just know that there is connection. We  
7     don't know whether it's -- we don't know what that connection is, we don't  
8     even know if it's electrical or physical. We just tap an arrow to show that  
9     operative connection.

10            And indeed we know from the '828 Patent that there -- the '828, the  
11     Petitioner focuses on the fact that there's a line between the processor and  
12     this -- in Figure 2A there's a floppy drive within the '828 Patent. But, you  
13     know, the interesting thing there is that the floppy drive itself, the floppy  
14     drive connection is one that in computer equipment, that vault that, you  
15     know, was existing at the time the '828 patent, it wasn't the one that was  
16     within a circuit board.

17            I don't know, I may be getting a little bit old, but I personally  
18     remember the 3.5-inch floppy drives. And there was a big cable -- and that's  
19     illustrated on image from Exhibit 2010. And this was a cable that -- this  
20     specific one would connect to a 5.25-inch floppy drive at the top. And then  
21     there's the other -- the connection in the middle here would connect to the  
22     3.5-inch floppy drive.

23            But in any event, like cables are specifically, you know, one type  
24     of non-conductive lead or trace, that's illustrated in Figure 2A, that we know  
25     that is, you know, shown by lines. So the lines in Figure 2A, contrary to  
26     what Petitioner says, some of these lines are not only by conductive leads or

1 traces.

2 Turning to Slide 18. The prosecution history, it -- the lines  
3 -- there's no discussion that the lines in Figure 2A depict conductive leads or  
4 traces specifically. Those are just exemplary structures from this portion  
5 from the prosecution history, which we discussed earlier. And as we  
6 mentioned there are a few alternative examples that are outside the  
7 conductive leads or traces.

8 Petitioner keeps on talking about coaxial cables, but the point that  
9 we were making wasn't specific to coaxial cables but cables generally. And  
10 this '853 Patent that was prior art, it showed a connection via a coaxial cable.  
11 We also have another patent, proper patent, this '981 Patent that illustrated  
12 satellite connections. You'll see -- or they were on Slide 20.

13 There's a connection to the satellites that -- on the left-hand side,  
14 between the device and the satellite on the left-hand side. And on the right-  
15 hand side, you also see a connection by a wired LAN interface 29. So at the  
16 time of the patent, you know, there were non-physical, non-electrical  
17 connections, nothing in the prior art.

18 JUDGE HOANG: Counsel, I understand you're saying that there's  
19 other ways to send data from one component to another. I think the point  
20 Petitioner might be trying to make is that in this specific type of packaging,  
21 this digital camera, that these two components of -- a skilled artisan would  
22 understand that these two components are going to be connected by  
23 conductive leads or traces as opposed to using Wi-Fi or these different types  
24 of cables, which seem to be in different types of devices. So, you know, in  
25 the '853 Patent, you point out that's a computer and a separate camera and a  
26 monitor.

1           Then in the '981 Patent that's a, you know, satellite system with  
2   personal computers. How do you respond to Petitioner's position about, you  
3   know, this is for a digital camera, a security --

4           MR. ATKINSON: I would say that we just don't know because  
5   just no information given about how the connection is made. All we know is  
6   -- the only thing that Glass is saying is that -- Glass is frankly agnostic as to  
7   how the connection is made between the imager and digitizer and the frame  
8   store. All it cares about is that the information gets from imager and  
9   digitizer to the frame store. But it doesn't talk about how that connection is  
10   made at all. So we just don't know what the connection is within Glass.

11           I mean, you know, could it be by conductive leads or traces? I  
12   mean, possibly, but we don't know. There's just no information from Glass  
13   on how the connection is made. All we have is a possibility. But, you  
14   know, there's just no information to know what's happening here.

15           And Rieger, on this point I think, is very similar to Glass because  
16   there's a protective -- a protected section that's encompassing all these  
17   devices. But all we know is that -- this is Slide 22 -- we have a CCD sensor  
18   that's sending information to a CPU, which is then sending that information  
19   to RAM. So, you know, we have an intermediary component in here with  
20   the CPU that's sitting between the RAM and the sensor.

21           But regardless, you know, all we have is arrows and -- but we don't  
22   -- I mean, in Rieger, it's the description of how these components are. The  
23   description of Figure 3 is very short. All it's focused on is that there's an  
24   operative connection between the CCD sensor and, you know, these two  
25   other components, CPU and RAM.

26           There's no details on what the connection is. So we know that

1 there's an operative connection to provide data indirectly from the CCD  
2 sensor to RAM via the CPU. But we don't know whether it's electrophysical  
3 connection or otherwise, right? So I think that's the point we made on Slide  
4 23.

5 The next point is, you know, monitoring of the tight coupling.  
6 And so on Slide 24, we see Glass again. Glass does not monitor the  
7 interconnection between the sensor and the memory itself. What it does is  
8 Glass monitors this -- you know, there's this tamper resistant and responsive  
9 packaging for -- that's shown or visible on Figure 3 of Glass.

10 And you see a bunch of components within it, which includes the  
11 optics sensor and the frame store. But you see a bunch of stuff here. Like,  
12 in this portion of Figure 3, there's this control logic, there's a multiplexer,  
13 and there's this comm interface that sits partially within this package. And if  
14 you look at Figure 3, it's full of that.

15 So there's a whole bunch of components there within this tamper  
16 resistant and responsive packaging. But there's nothing that's specifically  
17 monitoring the connection between the -- I'm sorry, the imager and digitizer  
18 42 and the frame store itself.

19 JUDGE AMUNDSON: This is Judge Amundson. On your point  
20 here, what if the tamper resistant packaging in Figure 3 only surrounded two  
21 components, the imager and digitizer and the frame store, in that  
22 hypothetical situation, would you say that it satisfies the claim language?

23 MR. ATKINSON: In so long as it was making sure that the  
24 connection was undisturbed, then potentially. But the issue is that we need  
25 to make sure that the connection is undisturbed. What's happening with the  
26 tamper resistant packaging is making sure that there's not been -- you know,

1 that the packaging is okay, but it's not simply monitoring anything within the  
2 package or no connections within the package. It's just monitoring the  
3 package itself.

4 JUDGE ARBES: Counsel, I think you had mentioned a protective  
5 shield over those two components as an example of what we might be  
6 talking about here. Wouldn't Judge Amundson's example of a tamper  
7 resistant packaging over just those two components -- wouldn't that be such  
8 a device?

9 MR. ATKINSON: Right. So if the device is specifically situated  
10 between the two interconnected components, such that the interconnection  
11 between those two devices is monitored and ensured to be secure, then that  
12 would be such a device, yes. And as we previously talked about, you know,  
13 here's -- this is where the specification talks about the internal security 14  
14 and it is monitored to protect the integrity of the tight coupling.

15 The system checks that the security system 14 to make sure to  
16 determine whether there's been any violations. If there is a violation, then  
17 that violation is appended to the image. So the violation happens when the  
18 coupling -- or the protection of the coupling provided by internal security 14  
19 has been violated.

20 JUDGE HOANG: Counsel, I'm going to get back to a little bit of  
21 claim construction on this limitation because I think, you know, whether or  
22 not Glass and Rieger reach this limitation will be based on what the ultimate  
23 claim construction is. What do you make of the District Court's tentative  
24 claim construction that this limitation should be construed as determining  
25 whether physical access has been gained to the connection between said  
26 memory and said sensor -- oh, so I'm sorry, that was actually Adobe's, the

1 District Court's tentative claim construction is determining whether physical  
2 access has been gained to the coupling between set memory and set sensor?

3 MR. ATKINSON: Let me go back. So I think the issue is that  
4 -- physical access isn't the only thing that can result in a violation. What we  
5 need to make sure is that the coupling hasn't been accessed or disturbed,  
6 whether that access is by, you know, physical means or other means. What  
7 we want to make sure is that the internal security -- makes sure that the  
8 information that slowing hasn't been accessed or disturbed.

9 So if there was a way where you could intercept that information  
10 without gaining physical access, that would be a problem whether physical  
11 access happens or not. So I think what the issue is that we will make sure  
12 that the physical coupling has not been accessed or disturbed, whether  
13 physical access has been feigned (PHONETIC).

14 JUDGE HOANG: So you're disagreeing with the District Court's  
15 tentative claim construction, and your construction is a little bit narrower  
16 because you actually are requiring some kind of breach.

17 MR. ATKINSON: Yeah. I think it is -- I think it should be a bit  
18 narrower than what the District Court construed. Because we didn't need to  
19 make sure that the -- that's -- physical coupling between the memory of the  
20 sensor set that hasn't been accessed or disturbed. So it's narrower in one  
21 sense but also broader in another sense. Because if it was accessed or  
22 disturbed, we want to make sure that it's directed to the physical coupling if  
23 that makes sense.

24 JUDGE HOANG: Yeah. I guess the -- on the POR on page 11 in  
25 your claim construction section, the proposed construction from Patent  
26 Owner is determining whether the physical coupling between the memory

1 and the sensor has been accessed or disturbed. So this seems to be a little bit  
2 broader than only disturbed, right? This says either accessed or disturbed.

3 MR. ATKINSON: Only accessed and disturbed would imply that  
4 you're able to -- you know, even without access, you're able to provide false  
5 information, which would be undesirable.

6 JUDGE HOANG: Right. But would this construction only require  
7 access to the physical coupling as opposed to disturbing the physical  
8 coupling? Because it uses the word "or."

9 MR. ATKINSON: Right. So if you access the physical coupling  
10 or disturb the physical coupling, either one -- if you're able to access without  
11 -- if you're able to disturb without even physically accessing it, then that  
12 would be a violation under our proposed construction. Under Petitioner's  
13 construction, it wouldn't be because you only have a violation when there's  
14 been physical access, regardless of whether it's been disturbed.

15 JUDGE AMUNDSON: Counsel, can I ask your view? Looking at  
16 pages 12 to 13 of the District Court's tentative order, I'm wondering if the  
17 District Court viewed these as different, really? On page 12, for instance,  
18 the court says, as discussed above, the tight coupling between the memory  
19 and sensor is physical. Thus, as Adobe argues, monitoring involves  
20 determining whether the physical coupling has been accessed or disturbed.  
21 And that mirrors your construction. How do you view that language in the  
22 District Court's tentative order?

23 MR. ATKINSON: Yeah. I don't think that the District Court was  
24 necessarily focused on that specifically. But I think that -- given the Court's  
25 language, I think that probably accessed or disturbed would be more  
26 accurate. I just don't think that is -- I don't think that the District Court was

1 focused on that issue specifically when it was making those statements.

2 JUDGE HOANG: Counsel, you have less than five minutes. But I  
3 also have a question. Is access merely being able to get to the physical  
4 connection, is that enough for access?

5 MR. ATKINSON: Well, it depends on what "get to" means. But  
6 if you're able to access it in order to provide false information, then that  
7 would be a violation. But if you're able to disturb it, in some way hamper or  
8 do something that even if you're not providing information, changes the  
9 information, then that would also be a violation. That I think that's why  
10 "disturbed" is important.

11 JUDGE HOANG: So on the access point, wouldn't breaking into  
12 the housing of the camera, which houses the physical coupling, wouldn't that  
13 be accessed?

14 MR. ATKINSON: It would be both accessed and disturbed, I  
15 think, yes. Because, you know, we -- well, I guess if you broke into the  
16 physical housing, you wouldn't necessarily disturb it, but you would access  
17 it. If you broke in -- if you disturb the physical connection without -- you  
18 know, if you're able to hinder the physical connection in some way without  
19 access, then that would also be a violation, I think.

20 Anyway, moving on to Slide 28, as, you know, moving to Rieger.  
21 Rieger and Glass are very similar because Rieger, as I mentioned in Slide  
22 27, has this protective section. So it's very similar to Glass where you have  
23 this protective section surrounding us with, you know, plurality of  
24 components. But, you know, it's not specifically monitoring the connection.  
25 In fact, you know, there's not -- there are direct connection in Rieger  
26 between the sensor and the RAM.

1           The final issue -- and I don't think that -- you know, this probably  
2 will take a lot of time. So in Glass, the issue is that you're only writing to a  
3 log file, but there's no guarantee that any user will ever -- the log files, you  
4 know, they're used a lot in computers. And a lot of times people don't look  
5 in log files, hardly ever, if ever.

6           And so, you know, there's no assurance that anyone will ever see  
7 what's written to the log files in Glass. And, you know, the other issue in  
8 Glass is that the person that's authenticated -- that's doing the image  
9 authentication probably isn't the user that's -- that would have access to a log  
10 file. Because the administrator to the system might have access to the log  
11 file, but the administrator wouldn't necessarily be the person that would be  
12 trying to do an image authentication.

13           And, you know, the reverse is also true. The person that is doing  
14 the image authentication or taking the image that's being authenticated,  
15 there's no -- there'd be no reason why that person would necessarily have  
16 access to the log file. And Rieger is actually very silent as to how, if at all,  
17 results are communicated to the user.

18           It seemed like in Petitioner's discussion -- in the patent -- in the  
19 petition, they're focused on the smiley face and these frowny face emoticons  
20 that are shown in Figure 7 of Rieger. But that -- those are just merely  
21 illustrations of the process and not how anything is actually done within the  
22 device. So there's no showing that, you know, these smiley and frowney  
23 faces would be communicated to the user.

24           And frankly, Rieger doesn't say how or if the results are  
25 communicated to the user at all. I mean, the Petitioner seems to now be  
26 taking more of an inherency argument. But I don't think -- I think if you

1 look back at the petition, inherency wasn't the argument that Petitioner was  
2 making whole the way through.

3 In fact, I think the -- I think arguing that it's inherent is something  
4 new that we're only hearing about today. And Serret-Avila briefly is mainly  
5 directed to when there's been a failure, it communicates -- it takes a  
6 defensive action. But there's nothing in Serret-Avila that talks about  
7 communicating anything when there's no -- when everything is "ok."

8 Serret-Avila is -- it also notably isn't directed specifically to  
9 imaging. It deals with lots of -- it deals with audio files. It deals with video.  
10 So it isn't clear how -- if there was any -- it basically authenticates each  
11 block separately. So the image might be composed of several blocks and  
12 there's nothing to indicate to a user which block would be -- would result in,  
13 you know, being "ok" or "failure."

14 Basically, you would need all the blocks to be "ok." In order to  
15 view an image in a video, you know, it kind of talks about doing kind of this  
16 real time authentication. So you might be able to kind of guess roughly  
17 based on when the video would stop, when the -- when a violation occurred.  
18 But, you know, you don't know what's happening as you're going with the  
19 specific block. So there's nothing -- there's no "ok" signal, specifically in  
20 Serret-Avila that's communicated to the user. And all that happens is that  
21 whenever there's a violation, it takes a defensive action.

22 And with that, I think I'll reserve the remainder of my time.

23 JUDGE HOANG: Great. You're just under three minutes over the  
24 allocated 53 minutes. So you'll have a little bit over four minutes for your  
25 surrebuttal.

26 MR. ATKINSON: Thank you.

1 JUDGE HOANG: Petitioner, you have about a little over nine  
2 minutes for your rebuttal time. You may begin when you're ready.

3 MR. DAY: Thank you, Your Honors. Just a few points. First, on  
4 this question about expertise -- and is the patent about security or about  
5 images -- I wanted to just refer you to recall the only thing about security in  
6 the '828 Patent is that you apply a signature protocol. On column 7, lines 25  
7 through 26, it says the signature protocol used is the commercially available  
8 MD5. It could be something else.

9 The patent is talking about using commercially available off-the-  
10 shelf security software. And the rest of the patent is about a digital camera  
11 and how you might employ that. So it's not a -- this is not a security patent.  
12 It's applying basic security concepts in the context of camera. And then the  
13 claim stretches that out to say, well, it could also be audio or other types of  
14 data streams.

15 Talking again about the monitoring, I'd refer you to our Slide 35.  
16 Slide 35 has the key phrases from the prosecution history. First, the  
17 applicant said, you know, what the limitation means is that a signal is  
18 generated if the device that prevents physical access is broken. The  
19 applicant is also talking about the tight coupling and said, in accordance with  
20 the present invention, the claimed tight coupling requires that the  
21 connections between the sensor and the memory not be physically  
22 accessible.

23 These two statements go together perfectly. It's tightly coupled  
24 because the user can't physically access it. And we're going to monitor to  
25 make sure that if somebody does break into the camera, a signal is  
26 generated. So our view of this is based directly on the intrinsic evidence.

1 And these two statements, I think, clearly support each other in our position.

2 JUDGE ARBES: Counsel, if you can go back to your Slide 33 for  
3 a moment. And I'd like to hear your response to Patent Owner's argument  
4 that the words "the device" in that sentence are really referring to the internal  
5 security system 14 and not the camera only. Can you respond to that?

6 MR. DAY: Yeah. That's wrong, Your Honor. Because if you  
7 look at the prior sentence -- so on Slide 33, the prior sentence is talking  
8 about flowchart 4A, step 59. That's a decision block in which it is  
9 determined whether internal security has been compromised. When it uses  
10 the word internal security, this is just a yes, no. This is a decision that has  
11 just been made. It's not talking about a device there. So in the next  
12 sentence, we're back to talking about the patent, which is describing a  
13 camera.

14 JUDGE ARBES: Well, Counsel, if we can take a look at column  
15 5, starting in line 44 of the patent, which says "independent of the compass  
16 status, processing continues 58 with a check 59 of the internal security  
17 system 14. If there is a breach of security 60 the violation is recorded 61."  
18 Doesn't that support Patent Owner's view that 14 is a device or system that is  
19 checked?

20 MR. DAY: There is an internal device system that is checked.

21 JUDGE ARBES: Okay.

22 MR. DAY: That's true. It doesn't describe that -- there's no  
23 description of that internal device system, none. And a system that checks  
24 internal security is something that would determine the security of the  
25 internals of the camera. That's consistent with the file history that I showed  
26 you.

1           Also, if you look at Figure 2A, I just want to point out, internal  
2 security 14 is also described just as the yes, no, was internal security violated  
3 or not, right? Because Figure 2A is a diagram of the camera, on the right-  
4 hand side are sort of inputs that gets sent to the processor. Internal security  
5 14 is not described as a system. This is just the result of -- whatever that  
6 system is, it's the result; it's fed to the processor.

7           Now, if it was something that had to do this -- the line between the  
8 processor and the floppy drive, that's what the applicants say in file history,  
9 it's tightly coupled. There's no indication anywhere in the patent. And you  
10 would expect here in Figure 2A, if internal security was all about that  
11 connection, you would think there'd be some evidence in the patent to say  
12 so. There's actually -- I mean, we're very far afield from the patent. There's  
13 no discussion in the patent specification itself of that connection, much less  
14 some system that is monitoring that connection.

15           So Counsel did his best to try to explain what that might look like.  
16 There is no disclosure in this patent of a system that specifically is  
17 monitoring a connection between a sensor and a memory. Again, there's not  
18 even a discussion of that connection.

19           JUDGE ARBES: But there's also no disclosure of assessing the  
20 internal security of the device as a whole, in your view, right?

21           MR. DAY: Well, I think that's true, there's no detail. The words  
22 internal security to me mean assess the security of the internals of the  
23 camera. So I think -- I don't completely agree with you, except that I  
24 completely agree there's no detailed description of any internal security  
25 system. And because of that, we look at file history, and we think file  
26 history is very clear how you monitor internal security. You generate a

1 signal if somebody broke into the camera.

2 Okay. Just a couple of more things. And Counsel, so now we're  
3 talking about the "okay" signal and the "error" signal. And Counsel said,  
4 sure, computers generate lots of log files and nobody ever looks at them.  
5 This is not any log file. Glass says this is a log file that contains irrefutable  
6 evidence if required. Glass is telling us that someone might want to look at  
7 that log file to determine if a particular figure -- sorry, a particular image  
8 was authentic or not.

9 Counsel also talked about how the user who took the picture might  
10 not be the same person who's trying to determine if the image is authentic. I  
11 think that could be true. It doesn't matter because the claim refers to a user.  
12 And at that point in the claim, it's whoever it is that's trying to determine if  
13 the image is authentic or not. In Glass, that very well could be some system  
14 administrator who's trying to determine if fraud was committed or not.  
15 That's why you create this log file to create irrefutable evidence of the  
16 transactions.

17 JUDGE HOANG: Petitioner, to the same limitation but addressing  
18 Rieger, Patent Owner asserted that -- this is Limitation 1H, asserted that  
19 Petitioner's position has changed from the petition to its arguments now,  
20 which seem more like inherency or disclosure type of arguments. Where in  
21 the petition did you make these arguments?

22 MR. DAY: So it's not inherent, and I don't want to leave that  
23 impression. What we said is in the petition, in the section on Rieger talking  
24 about these limitations, we said, there'd be no point in conducting the  
25 integrity test if you don't learn the result. That's, I think, where we talked  
26 about. That's why a person of ordinary skill in the art would understand that

1 based on Rieger, you would inform someone conducting the integrity test,  
2 that it -- certainly, that it failed, right?

3 Rieger, again, is all about evidence to be used in court. So you run  
4 the integrity test to determine whether the image is authentic or not. I think  
5 in our petition and certainly in the expert declaration, we said, no point in  
6 running the test unless you get that result. Showing a positive result would  
7 confirm that the image can be used as evidence. So it's not inherent. What I  
8 would point you to, though, is the discussion in Rieger where it says a user  
9 can determine by comparison. What I'm saying is that language tells me, I  
10 learn the result of the comparison.

11 Thank you, Your Honors.

12 JUDGE AMUNDSON: This is Judge Amundson. I had a question  
13 about the Markman hearing in the District Court. And it says that in another  
14 case, we had a situation where the judge -- the district judge gave a  
15 preliminary claim construction before the Markman hearing. And at the  
16 Markman hearing, the judge said, yes, the court maintains the preliminary  
17 construction or not. Did something like that happen at your Markman  
18 hearing?

19 MR. DAY: I do not believe so. I know that there were open  
20 questions. What I don't remember specifically is if with regard to any of the  
21 particular constructions, he said, we're just going to stick with this. The  
22 other thing, Your Honor, that might color this is I think there were a few  
23 constructions we agreed not to argue. They're not the ones that we're talking  
24 about today. So I believe -- I do not believe that with regard to the  
25 constructions we're talking about today, the court said, I'm going to stick  
26 with these, but I just -- I'm not positive about it.

1 JUDGE AMUNDSON: All right. Thank you.

2 JUDGE HOANG: Okay. Thank you. So we took about an extra  
3 minute. So Patent Owner, I'm going to add an extra minute to your  
4 surrebuttal time, so that will be a little bit over five minutes for you. And  
5 you can begin whenever you're ready.

6 MR. ATKINSON: So the first thing I'd like to address is what  
7 Petitioner said that '828 Patent was dealing with off-the-shelf security. I  
8 think that's just not -- that's not true. I think what's actually happening is that  
9 it's dealing with an off-the-shelf sensor that's modified to provide additional  
10 security to the '828 Patent.

11 So to accept that there's this division between, you know, image  
12 coding and security within the '828 Patent, what the off-the-shelf component  
13 is -- the off-the-shelf part is the image coding, i.e., the sensor is -- you know,  
14 for example, it might be making these JPEG images which are then have  
15 -- that are hashed right, this additional security, from -- taken from a  
16 parameter to secure the image. But the JPEG coding itself, that's -- that'd be  
17 off-the-shelf.

18 So the off-the-shelf piece that Dr. Xiong would -- basically, Dr.  
19 Xiong's imaging -- or image coding experience, that's the off-the-shelf piece  
20 in the context of the '828 Patent. What's unique and added in the context of  
21 the '828 Patent is the - all the security aspects dealing with how you're  
22 providing this additional information to secure the image from these  
23 parameters and then overlaying that parameter that's in a secure way to  
24 encode the image.

25 That's a security detail that's provided by, you know, security  
26 experience which has -- I previously mentioned, Mr. Davis has a great deal

1 of security experience; and Dr. Xiong has little, if any.

2 Second, regarding the monitoring issue, I think that the prosecution  
3 history is clear that when a violation occurs, what's happening is that the  
4 connection -- it's determining that the connection between the sensor and the  
5 memory has been accessed or disturbed. And it's not just whether the  
6 camera as a whole has been accessed or disturbed. I don't think there's  
7 anything within either the specification of the '828 Patent or the portions of  
8 the prosecution history that we've heard today that talks about monitoring  
9 the whole camera.

10 JUDGE ARBES: But Counsel, what are we to take in your view  
11 from the situation where you said that there may be nothing in the  
12 specification talking about monitoring the integrity of the camera as a whole,  
13 the word internal? But there's also no specific examples of monitoring the  
14 integrity of that specific connection between the two components? How are  
15 we to deal with that in your view?

16 MR. ATKINSON: Well, I think what's happening is that the  
17 internal security at all times within the schedule of the specification is it's  
18 making -- the internal security is directly aimed at ensuring that the  
19 connection between the sensor and the memory is secure. And so, like, there  
20 isn't a focus on securing any other portion of the camera.

21 I mean, there's just -- there's no discussion of security and other  
22 components at all. So I think, that's -- that'd be extraneous, you know, to the  
23 specification. There's really no discussion of that in the prosecution history  
24 either, in my view. I think that's all I wanted to cover.

25 JUDGE HOANG: Okay. Then Counsel, thank you for appearing  
26 today and for answering our questions. We'll take this case under

- 1 advisement and issue our decision in due course.
- 2 (Whereupon, the above-entitled matter went off the record at 12:08
- 3 p.m.)

IPR2024-01352  
Patent 6,757,828 B1

PETITIONER:

James L. Day  
Winston Liaw  
FARELLA BRAUN + MARTEL LLP  
jday@fbm.com  
wliaw@fbm.com

PATENT OWNER:

Bryan D. Atkinson  
Michael D. Saunders  
PRINCE LOBEL TYE LLP  
batkinson@princelobel.com  
msaunders@princelobel.com