UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

GOOGLE LLC,
Petitioner,

v.

SECURITY FIRST INNOVATIONS, LLC,
Patent Owner.

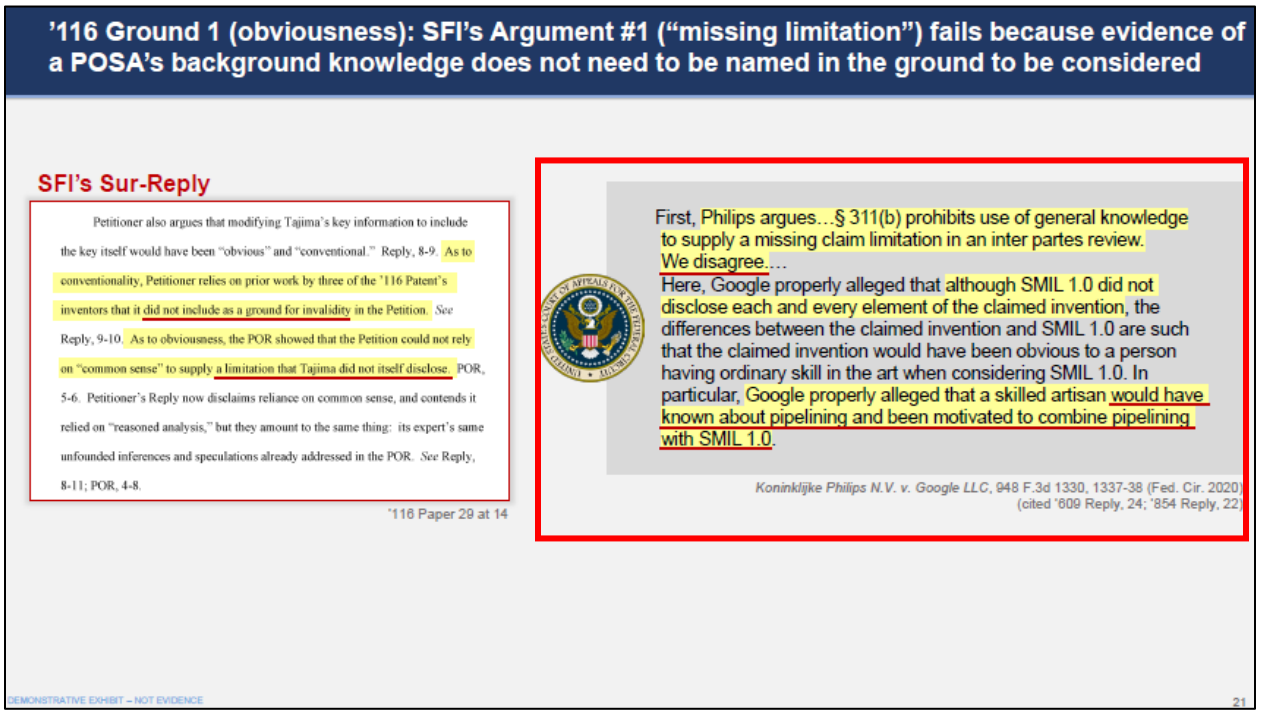
Case IPR2024-00215
Patent 10,452,854

PATENT OWNER'S OBJECTIONS TO PETITIONER'S DEMONSTRATIVE EXHIBITS

Patent Owner hereby submits its objections to Petitioner's demonstratives exhibits.

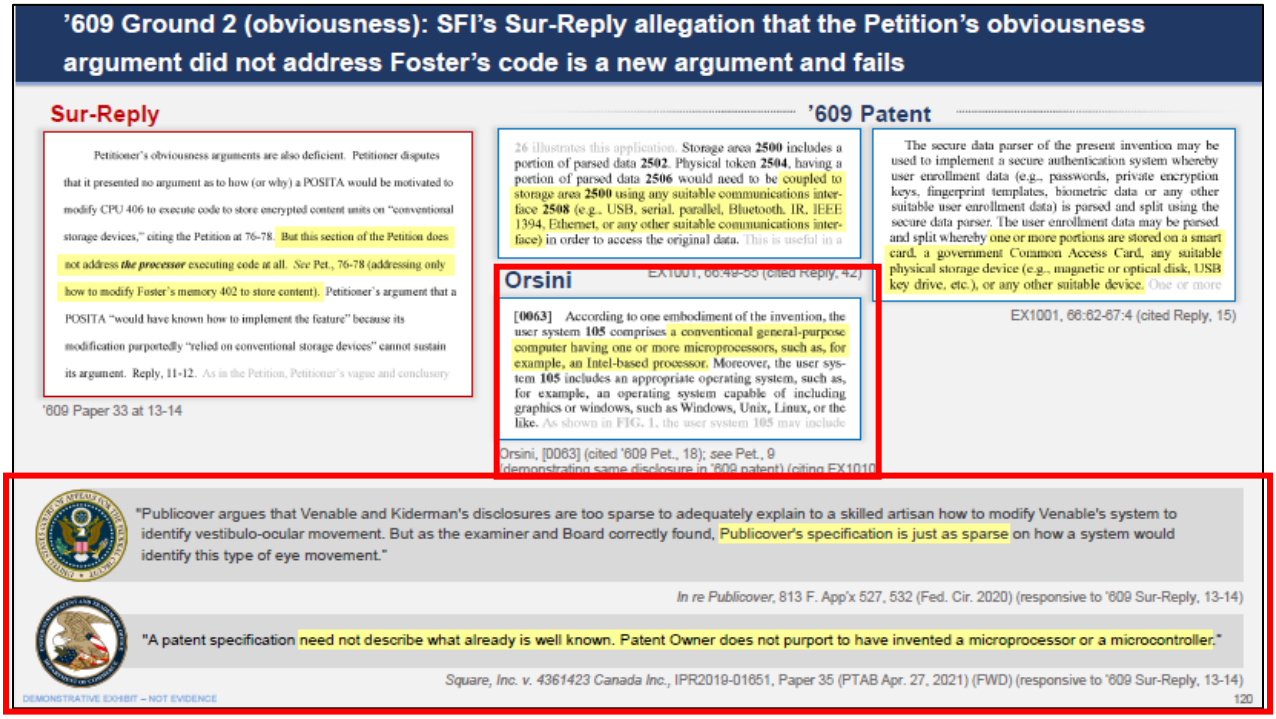
I. New Evidence Or Arguments

Slide 21:



Uncited case: Slide 21 cites a new case (*Koninklijke*) that is uncited in any briefing in IPR2024-00212 and presents a new argument that "evidence of a POSA's background knowledge does not need to be named in the ground to be considered" which is not present in briefing (*see* -00212 Reply, 8-11).

Slide 120:



Uncited cases, uncited evidence, and new argument: Slide 120 cites *Publicover* and *Square* which are not cited in papers, cites Orsini at [0063] which is not cited in the portions of the briefing addressing the limitation-at-issue (*see* -00214 Pet., 60-62, 72-78; Reply, 6-12), and presents new arguments not in any briefing that address "SFI's Sur-Reply allegation" and that the '609 does not contain any description of "executing code by a processor to perform … storing."

Slide 121:

'609 Ground 2 (obviousness): SFI's new Sur-Reply allegation that the Petition did not sufficiently address Foster's code for storing fails because SFI's Patent relies on conventional processors and code for storing

'609 Patent

According to one embodiment, the transaction engine **205** also transmits a confirmation message to the user. Although the signing process **1100** is disclosed with reference to its preferred and alternative embodiments, the invention is not intended to be limited thereby. Rather, a skilled artisan will recognize from the disclosure herein, a wide number of alternatives for the signing process **1100**. For example, the vendor may be replaced with a user application, such as an email application. For example, the user may wish to digitally sign a particular email with his or her digital signature. In such an embodiment, the transmission throughout the signing process **1100** may advantageously include only one copy of a hash of the message. Moreover, a skilled artisan will recognize from the disclosure herein that a wide number of client applications may request digital signatures. For example, the client applications may comprise word processors, spreadsheets, emails, voicemail, access to restricted system areas, or the like.

EX1001, 32:23-39 (responsive to Sur-Reply, 13-14)

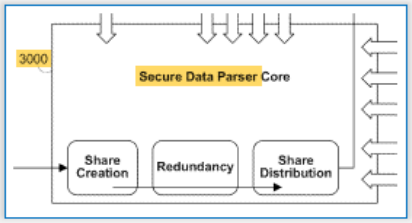
In addition, a skilled artisan will recognize that the cryptographic system **100** or the trust engine **110** may include the ability to recognize any type of devices, such as, but not limited to, a laptop, a cell phone, a network, a biometric device or the like. According to one embodiment, such recognition may come from data supplied in the request for a particular service, such as, a request for authentication leading to access or use, a request for cryptographic functionality, or the like. According to one embodiment, the foregoing request may include a unique device identifier, such as, for example, a processor ID. Alternatively, the

EX1001, 37:14-24 (responsive to Sur-Reply, 13-14)

known as "metadata", related to that password attempt. This circumstantial data includes information such as: the time at which the particular authentication instance took place, the network address from which the authentication information was delivered, as well as any other information as is known to those of skill in the art which may be determined about the origin of the authentication data (the type of connection, the processor serial number, etc.).

In many cases, only a small amount of circumstantial metadata will be available. For example, if the user is located on a network which uses proxies or network address translation or another technique which masks the address of the originating computer, only the address of the proxy or router may be determined. Similarly, in many cases information such as the processor serial number will not be available because of either limitations of the hardware or operating system being used, disabling of such features by the operator of the system, or other limitations of the connection between the user's system and the trust engine **110**.

EX1001, 38:62-39:14 (responsive to Sur-Reply, 13-14)



EX1001, FIG. 31 (partial) (highlighted) (responsive to Sur-Reply, 13-14)

FIG. **31** illustratively shows how the arrangement of FIG. **30** may be used when a write (e.g., to a storage device), insert (e.g., in a database field), or transmit (e.g., across a network) command is issued in application layer **3024**. At step **3100** data to be secured is identified and a call is made to the secure data parser. The call is passed through wrapper layer **3022** where at step **3102**, wrapper layer **3022** streams the input data identified at step **3100** into assembled data buffer **3008**. Also at step **3102**, any suitable share information, filenames, any other suitable information, or any combination thereof may be stored (e.g., as information **3106** at wrapper layer **3022**). Secure data processor **3000** then parses and splits the data it takes as input from assembled data buffer **3008** in accordance with the present invention. It outputs the data shares into split shares buffers **3010**. At step **3104**, wrapper layer **3022** obtains from stored information **3106** any suitable share information (i.e., stored by wrapper **3022** at step **3102**) and share location(s) (e.g., from one or more configuration files). Wrapper layer **3022** then writes the output shares (obtained from split shares buffers **3010**) appropriately (e.g., written to one or more storage devices, communicated onto a network, etc.).

EX1001, 72:33-54 (responsive to Sur-Reply, 13-14)

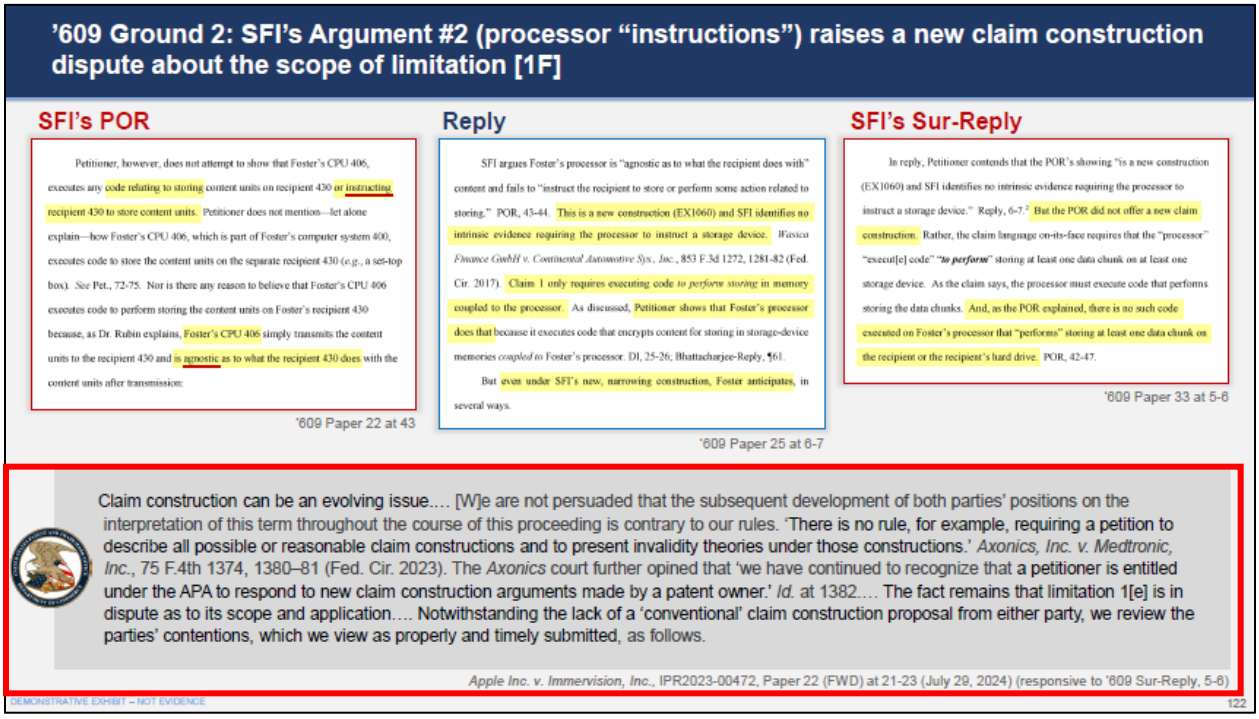
sic: "Secure data parser 3000"

DEMONSTRATIVE EXHIBIT – NOT EVIDENCE

121

New argument: Slide 121 contains presents new arguments not in any briefing, which are purportedly "responsive to [the] Sur-Reply," that "SFI's Patent relies on conventional processors and code for storing."

Slide 122:



Uncited case: Slide 122 cites a new case (*Immervision*) "responsive to [the] '609 Sur-Reply" that is not cited in any briefing.

Slide 125:

'609 Ground 2: Because SFI did not raise Argument #2's new claim construction pre-institution, Petitioner's reply was permitted to prove that Foster meets or render obvious under SFI's claim scope

Institution Decision

C. Claim Construction

* * *

4. Limitation [1F]: "storage device"

Claim 1 recites "storing, in a memory coupled to the processor, at least one data chunk of the plurality of data chunks with data indicative of at least one of the distinct encryption keys on at least one *storage device*." Ex. 1001, 83:27–30 (emphasis added).

Patent Owner argues that the recited "storage device" is for long-term storage:

> [The skilled artisan] reviewing the '609 patent would not understand a "storage device" to encompass something like Foster's receiver (*e.g.*, a set-top box or a DVD player) because the examples of storage devices given in the '609—"magnetic or optical disk, USB key drive, etc."—are each devices primarily dedicated to long-term storage.

* * *

We note that claim 1 does not use the term "long-term." Nonetheless, we need not resolve whether the claim requires long-term storage at this stage of the proceeding because we disagree with Patent Owner that this feature distinguishes Foster. *See infra* § III.D.2.a.

'609 Paper 16 at 18-19

SFI's Dr. Rubin

A. So the word "agnostic" does not appear in the claims here…

'609 EX1099, 189 (cited Reply, 6)

SFI's POR

Petitioner, however, does not attempt to show that Foster's CPU 406, executes any code relating to storing content units on recipient 430 or instructing recipient 430 to store content units. Petitioner does not mention—let alone explain—how Foster's CPU 406, which is part of Foster's computer system 400, executes code to store the content units on the separate recipient 430 (*e.g.*, a set-top box). *See* Pet., 72-75. Nor is there any reason to believe that Foster's CPU 406 executes code to perform storing the content units on Foster's recipient 430 because, as Dr. Rubin explains, Foster's CPU 406 simply transmits the content units to the recipient 430 and is agnostic as to what the recipient 430 does with the content units after transmission:

No citations to '609 patent

Paper 22 at 43; *see also id.*, 42-56

"Barring argument and evidence in a reply directed to a new claim construction proposed by the patent owner would create opportunities for sandbagging by the patent owner in order to create an estoppel. A patent owner has the opportunity in a preliminary response to oppose institution on the ground that the claim construction relied on by the petitioner is incorrect, and the Board may adopt the patent owner's proposed claim construction and deny institution if the petition fails to demonstrate a reasonable likelihood that a claim would be unpatentable under the correct claim construction. See 35 U.S.C. § 314(a). The result would be that there would be no institution and no estoppel pursuant to 35 U.S.C. § 315(e). But if instead of raising the issue in a preliminary response, a patent owner sits on its strongest claim construction arguments before institution and then raises them in response after institution, a patent owner could obtain a favorable final IPR decision and an estoppel without the Board's reaching the merits of any invalidity arguments under the newly adopted claim construction.… We are reluctant to adopt a construction of the APA and the Board's rules that would permit such gamesmanship.

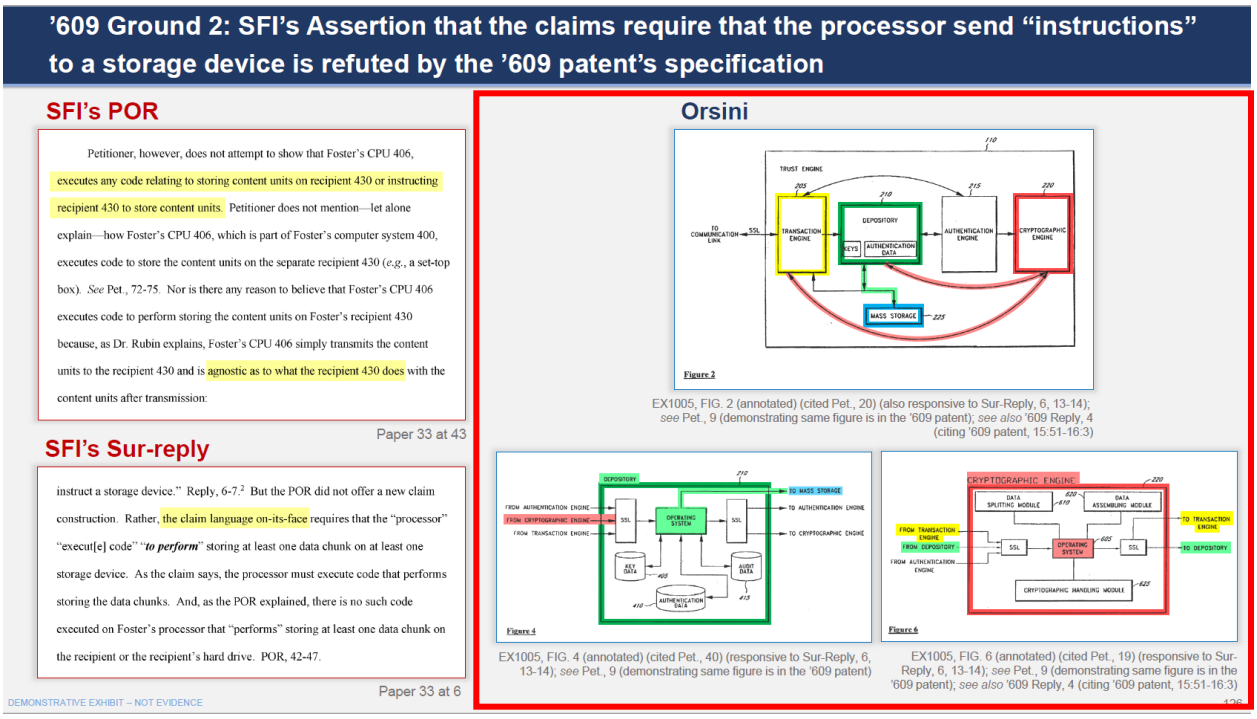
Axonics, Inc. v. Medtronic, Inc., 75 F. 4th 1374, 1384 (Fed. Cir. 2023) (cited '609 Reply, 4; '854 Reply, 14)

DEMONSTRATIVE EXHIBIT – NOT EVIDENCE

125

Uncited case: Slide 125 quotes *Axonics* citing "'609 Reply, 4; '854 Reply, 14," but the specified briefing relates to a different limitation and cites a different portion of *Axonics* for a different proposition.

Slide 126:



Uncited evidence and new argument: Slide 126 shows Orsini Figures 2, 4, and 6 to "respon[d] to [the] Sur-Reply" and citing Pet., at 9, 20, and 19, but the specified briefing relates to a different ground and does not present any argument that "SFI's Assertion that the claims require that the processor send 'instructions' to a storage device is refuted by the '609 patent's specification."

Slide 157:

'116 Grounds 3-4: SFI alleges AoNT causeses "error-propagation" but Rivest teaches that ways to minimize error propagation were already known to POSAs

SFI's POR

Petitioner additionally ignores the substantial drawback associated with using AoNT. As Dr. Rubin explains:

> Rivest also points out that "all-or-nothing encryption has ***terrible*** error-propagation properties" because if any pseudo-message block is damaged "then it is likely that ***every*** message block will be damaged." EX1034, 216. Accordingly, redundancy information should be included in any data set before it is transformed using the AoNT, a practice that is suggested in the '116 (*see* 77:23-36) but which would have to be added to Tajima.

'116 Paper 17 at 31

SFI's Sur-Reply

EX1034, 216. Petitioner admits that in its proposed combination, "individual transformed message blocks are kept ***and transmitted*** together," Reply, 20, the same action that Rivest discloses can lead to damage that would prevent inversion of the transformation. Thus Petitioner's Tajima-Rivest would require additional, failure-proof error-correction techniques not disclosed in either Tajima nor Rivest.

'116 Paper 29 at 11

Dr. Bhattacharjee

C. Response to Argument That AoNT Has Terrible Error Propagation Properties

51. Dr Rubin argues that a POSA would not have applied AoNT because Rivest says "all-or-nothing encryption has terrible error propagation properties" because if any message block is damaged "then it is likely that every message block will be damaged" (Rivest, 216). EX2033, ¶88. I disagree that a POSA would understand Rivest to be discouraging the use his own transform. Rivest is simply pointing out the importance or using reliable transmission means to reduce data corruption and/or to use error-correction techniques. EX1034, 216. Second, in the Tajima-Rivest combination the transformed data—both the first implementation where the key information is transformed, and in the second implementation in which the data fragment is transformed using the key information (see First Declaration, ¶¶189-190)—the individual transformed message blocks are kept together, transmitted and stored together. Thus, there is no "error propagation" in Tajima-Rivest.

'116 EX1111, ¶51 (cited '116 Reply, 19-20)

"Although the prior art that can be considered in inter partes reviews is limited to patents and printed publications, it does not follow that we ignore the skilled artisan's knowledge when determining whether it would have been obvious to modify the prior art.

Koninklijke Philips N.V. v. Google LLC, 948 F.3d 1330, 1337 (Fed. Cir. 2020) (cited '609 Reply, 24; '854 Reply, 22) (quoting 35 U.S.C. §103) (pre-AIA)

DEMONSTRATIVE EXHIBIT – NOT EVIDENCE

157

Uncited case: Slide 157 cites a new case (*Koninklijke*) that is uncited in any briefing in IPR2024-00212 and presents a new argument that "it does not follow that [the Court] ignore the skilled artisan's knowledge when determining whether it would have been obvious to modify the prior art" which is not present in briefing (*see* -00212 Reply, 8-11).

Slide 167:

SFI's Expert Admits Tajima's FIG. 13 Shows "Key Information"

SFI's Dr. Rubin

Q. So let me ask again. In Figure 13 there's encrypted personal information and key information on the key that was used in encrypting the personal information, correct?

A. I'm sorry. Go ahead, Nate.

Q. And the key information of that first key is shown by the two hash marks in Figure 13, correct?

A. When you say the two boxes that are shaded?

Q. Yes.

A. That represents information about the key that was used to encrypt the personal information.

Q. And if you look to Figure 11, it has a very similar figure, and it calls those two boxes key information. Do you see that?

A. Yes.

Q. And Figure 13, it's just left out that label. Do you see that?

A. The label is not there.

Q. Right. But the key information is what those two hash marks are in Figure 13, correct?

A. I think that's what is explained in the text, and I believe that's the case.

'116 EX1099, 172-173 (objections omitted)
(responsive to '116 Sur-Reply, 14)

DEMONSTRATIVE EXHIBIT – NOT EVIDENCE

167

Uncited evidence: Slide 167 quotes from Ex. 1099 at 172-173 that is uncited in any briefing and which is allegedly "responsive to [the] '116 Sur-Reply."

Slide 178:

"Patent Owner asserts that Petitioner's Reply brief "presents new evidence and arguments beyond the scope of a proper reply" and "[t]he Board should refuse to consider" it. Sur-reply 9–10. This generic objection to the entire Reply fails to provide adequate notice regarding which of Petitioner's theories and arguments Patent Owner contends are allegedly new and improper. See, e.g., Rembrandt Diagnostics, LP v. Alere, Inc., 76 F.4th 1376, 1383 (Fed. Cir. 2023) (rejecting generic objection to alleged new theories in reply as failing to provide adequate notice of which theories are allegedly new). Accordingly, we reject Patent Owner's request that we "refuse to consider" the entirety of the Reply. Where Patent Owner's Sur-reply raises more particularized complaints regarding Petitioner's allegedly improper new arguments, we address those complaints as appropriate below.

Life Spine, Inc. v. Globus Med., Inc., IPR2022-01599, Paper 39 at 24 n.10 (FWD) (PTAB)

"Mr. Hatch's testimony in paragraphs 53–55 is persuasive to support the argument for which Petitioner cites them and the mere fact that Mr. Hatch provides additional detail to support that argument does not amount to an improper incorporation by reference. Indeed, expert testimony is generally more persuasive when it does not merely parrot the arguments in the briefs, but provides additional detail supporting the argument for which it is cited, as it does here."

Life Spine, Inc. v. Globus Med., Inc., IPR2022-01599, Paper 49 at 45 (FWD) (PTAB)

"Patent Owner asserts that Petitioner's Reply "exceeds the proper scope of reply by explaining its protrusion theory for the first time via lengthy new testimony (Ex. 1072 ¶¶ 122–131), despite Mr. Drewry's original declaration never referencing the issue." Sur-reply 27 (citing Ex. 1002 (Drewry Decl.) ¶¶ 461–66). We disagree. We find that Petitioner's discussion of the protrusion problem is both a permissible expansion on its arguments made in the Petition, and response to Patent Owner. See Corephotonics, Ltd. v. Apple Inc., 84 F.4th 990, 1008 (Fed. Cir. 2023) ("'there is no blanket prohibition against the introduction of new evidence during an IPR,' provided it is an 'expan[sion] on and . . . fair extension of . . . [a] previously raised . . . argument' and has a 'nexus' (and is therefore responsive) to an argument made by the patent owner or the Board") (quoting Rembrandt Diagnostics, 76 F.4th at 1384–85) (alterations in original). The Petition identifies a concern with the actuator "stick[ing] out the far end of the central ramp," and Mr. Drewry's original declaration stated that the combination would "allow a surgeon to use a shorter actuator." Pet. 109; Ex. 1002 (Drewry Decl.) ¶ 462. As we discuss above, in attempting to rebut Petitioner's argument, Patent Owner misdescribed Petitioner's proposed combination. Under the circumstances here, we find that Petitioner's Reply and Mr. Drewry's Reply declaration appropriately elaborate on the Petition and respond to Patent Owner's counterarguments related thereto.

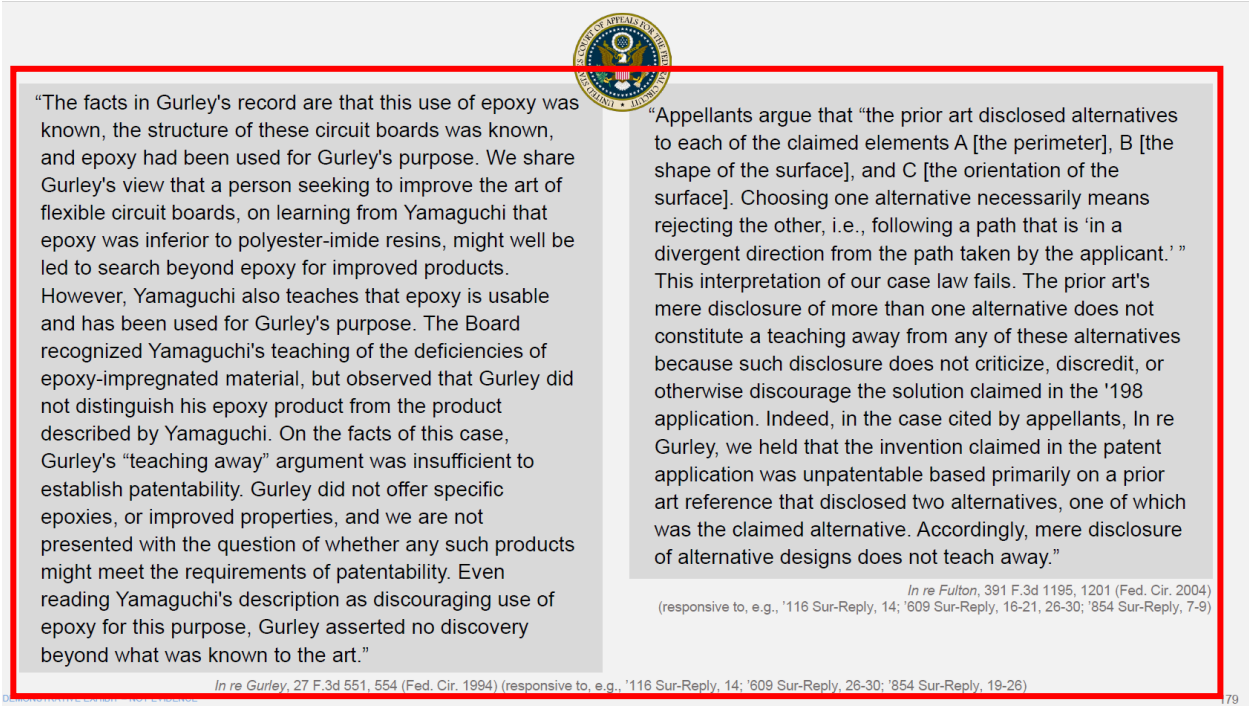
Life Spine, Inc. v. Globus Med., Inc., IPR2022-01599, Paper 39 at 95 n.20 (FWD) (PTAB

DEMONSTRATIVE EXHIBIT – NOT EVIDENCE

178

Uncited cases: Slide 178 quotes from several papers in *Life Spine*, which was never cited in any paper of record.

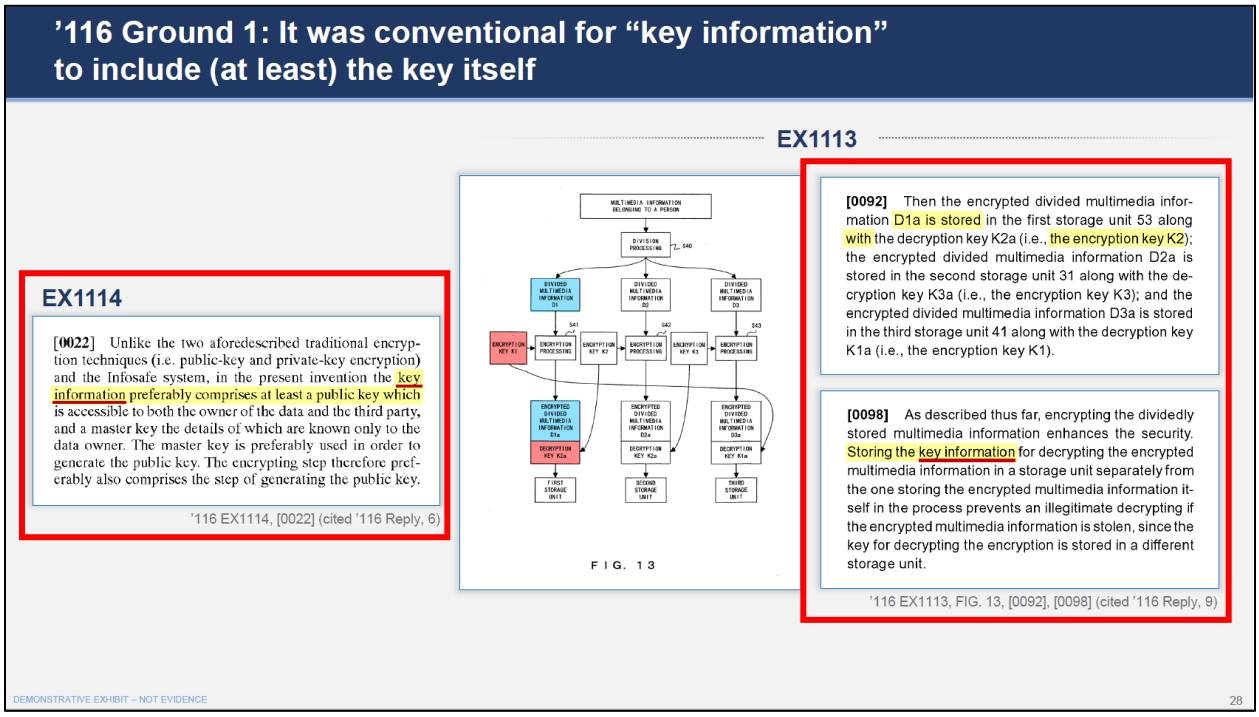
Slide 179



Uncited cases: Slide 179 quotes from *Gurley* and *Fulton* to "respon[d] to [the] '609 Sur-Reply," but neither case was ever cited or presented in any briefing of record.

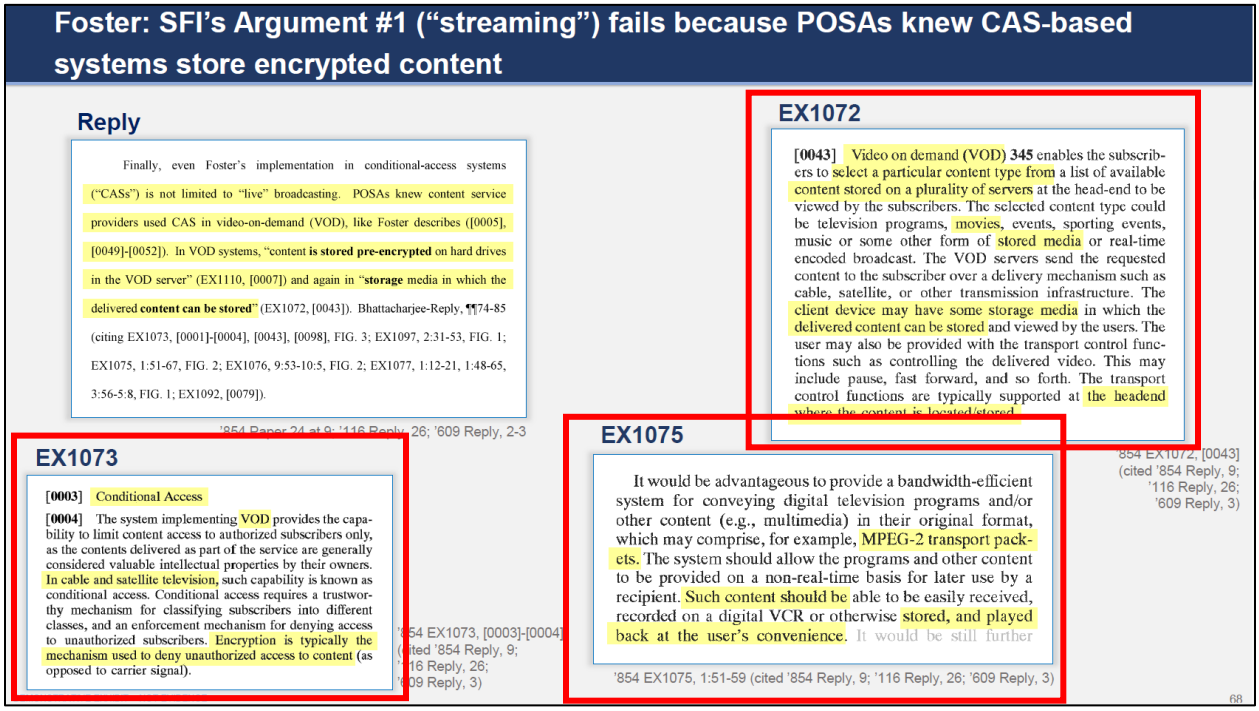
II. Evidence Incorporated-By-Reference In Briefing

Slide 28:



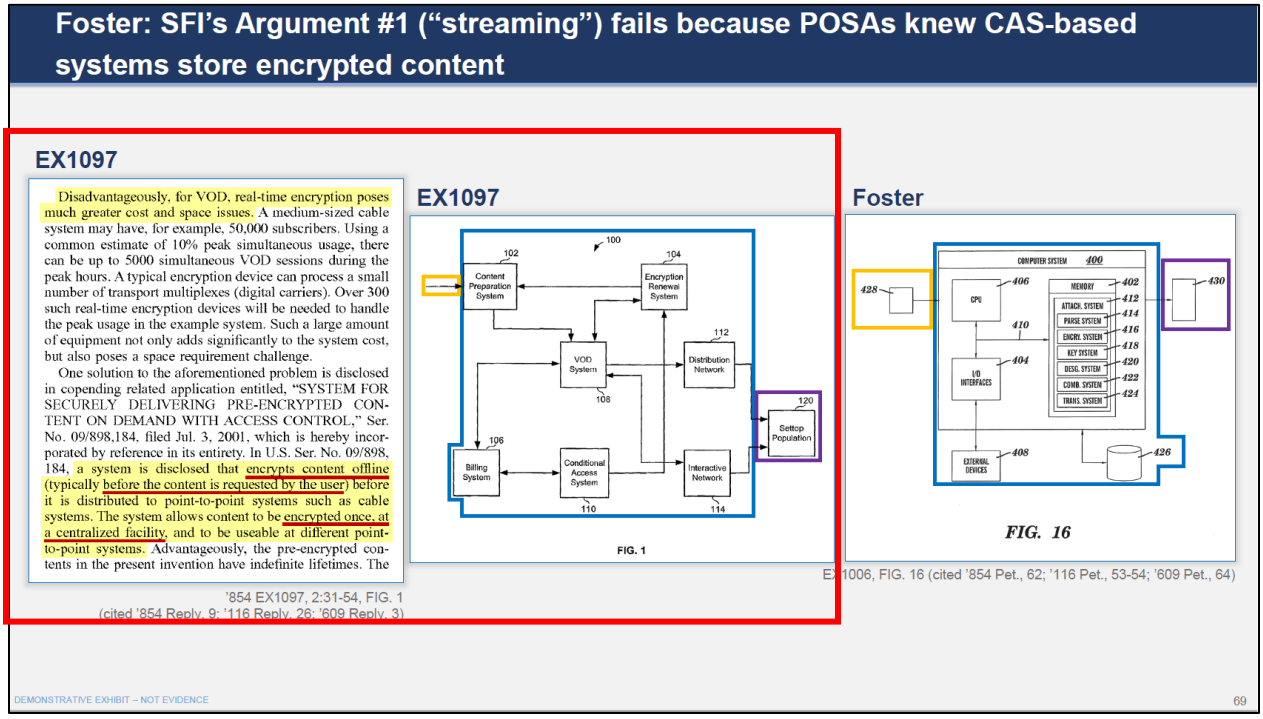
Evidence incorporated-by-reference: Slide 28 contains quotes from Ex. 1113 at [0092], [0098] and Ex. 1114 at [0022] that were only cited without explanation in the identified portions of the briefing (-00212 Reply, 6-9).

Slide 68:



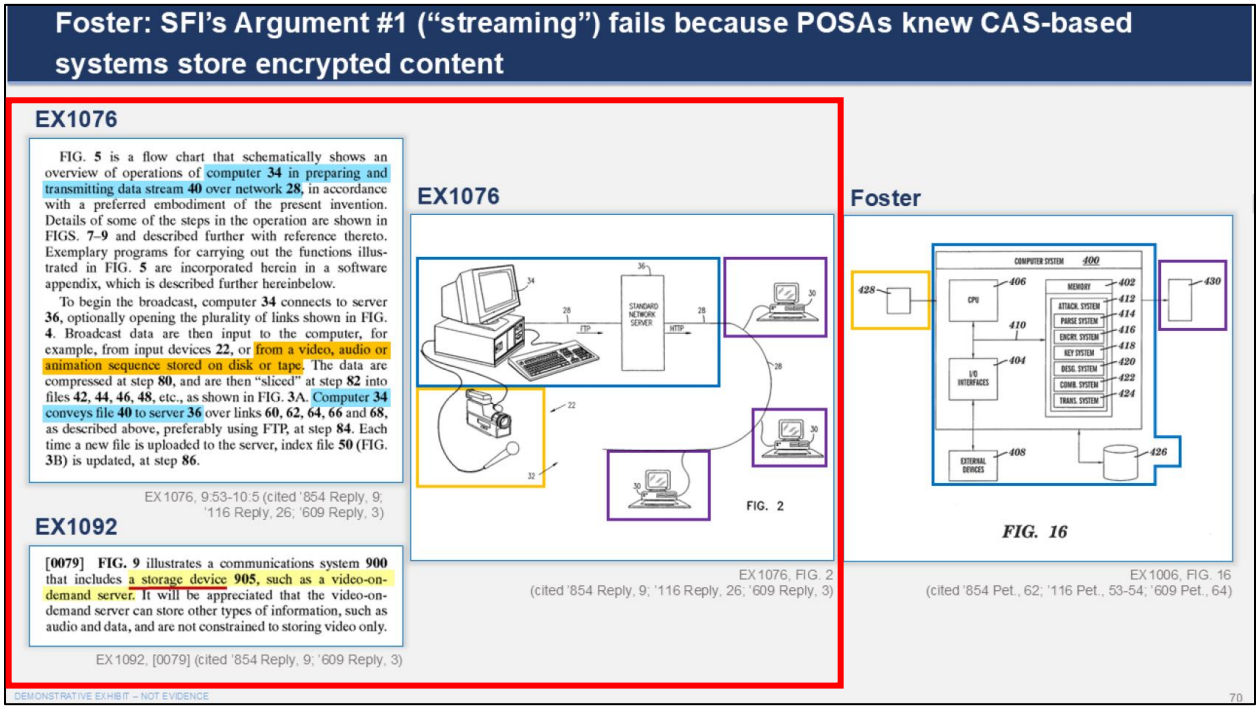
Evidence incorporated-by-reference: Slide 68 contains quotes from Ex. 1072 at [0043], Ex. 1073 at [0003]-[0004], and Ex. 1075 at 1:51-59 that were only cited without explanation in the identified portions of the briefing (-00212 Reply, 26; -00214 Reply, 2-3; -00215 Reply, 9).

Slide 69:



Evidence incorporated-by-reference: Slide 69 contains quotes from Ex. 1097 at 2:31-54 and Figure 1 that were only cited without explanation in the identified portions of the briefing (-00212 Reply, 26; -00214 Reply, 3; -00215 Reply, 9).

Slide 70:



Evidence incorporated-by-reference: Slide 70 contains quotes from Ex. 1076 at 9:53-10:5 and Figure 2 and quotes from Ex. 1092 at [0079] that were only cited without explanation in the identified portions of the briefing (-00212 Reply, 26; -00214 Reply, 3; -00215 Reply, 9).

Slide 75:

Foster: SFI's Argument #1 ("streaming") fails because Foster encrypts for a "program stream," which Foster says (and POSAs knew) is "generally used" "in fixed storage"

Reply

Consistent with its DRMS disclosures, Foster discloses processing datasets for an MPEG "program stream," which Foster says (and POSAs knew) is intended for storing "**in fixed storage**." Foster, [0073]; *see also* EX2014, 1 ("[p]rogram streams are **designed for**…**storage**"); EX1108, 1:65-2:31; EX1109, 1-9, 13); EX1072, [0002]-[0004], [0011], [0042]-[0043]; Bhattacharjee-Reply, ¶¶67-73; Rubin-Depo., 82-85 (admitting there are "different ways of encoding MPEG data" but he did not "discuss[] the distinctions"). Foster's text makes clear that Foster includes storage-based embodiments.

'854 Paper 24 at 8; '116 Reply, 26; '609 Reply, 2

SFI's EX2039

The MPEG-2 standard defines two ways to deliver packetized elementary streams: *program streams* and *transport streams*.

Program Streams

Program streams are designed for environments that are relatively error-free, such as local file storage. In a program stream, the PES packets are multiplexed and organized into units called *packs*. All of the PES streams in a program stream are synchronized to the same clock.

EX2039, 1 (cited '854 Reply, 8; '116 Reply, 26; '609 Reply, 2)

Foster

[**0073**] Once the encrypted key (and any optional identifier information and/or verifier) has been attached to PES packet **306**, the resulting PES unit **302** can then be multiplexed in two different system options. The first is shown in **FIG. 14** and is known as a transport stream. A transport stream is typically used in error-prone broadcast environments such as digital television. As depicted, transport stream packets **350**A-F are relatively small, and it generally takes multiple transport stream packets **350**A-C to contain a single video PES unit **302**. The second option is a program stream, which is shown in **FIG. 15**. A program stream is generally used in more reliable transmissions such as those with error correcting codes or in fixed storage. Unlike transport stream packets, however, a single program stream packet **360** can hold multiple video PES units **302** and **362**.

'854 EX1006, [0073] (cited '854 Reply, 9; '116 Reply, 26; '609 Reply, 2, 10, 15)

EX1108

and presented together in a coherent fashion. The program and transport streams may be recorded on or played back from a digital video disc (DVD), video tape, magnetic or optical disk drive or other suitable storage device. It should

EX1108, 2:1-4 (cited '854 Reply, 9; '116 Reply, 26; '609 Reply, 2)

DEMONSTRATIVE EXHIBIT – NOT EVIDENCE

75

Evidence incorporated-by-reference: Slide 75 contains quotes from Ex. 1108 at 2:1-4 that were only cited without explanation in the identified portions of the briefing (-00212 Reply, 26; -00214 Reply, 2; -00215 Reply, 8).

Slide 79:

'116/'854 Foster-Hayhurst: SFI's Argument #2 ("incompatibility") fails even if Foster were limited to real-time streaming because SFI's patents say (and POSAs knew) that distributed storage/delivery supports streaming

SFI's Sur-Reply

Foster's emphasis is avoiding delays to allow swift random access to content. As Petitioner's expert concedes, "synchronous transmission" of a series of packets and the keys used to encrypt them to "foster random access to content" at a (single) receiver was "sort of the whole invention in Foster." EX2034 [Bhattacharjee-Depo.], 32:20-23. The Foster-Hayhurst combination, however, would thwart these aims because applying Hayhurst's distribution regime to Foster would massively increase delays (the very thing Foster sought to avoid) and preclude real-time streaming and/or random access to content. *Id.*, 57-64. The synchronization of keys and content required by Foster is irrelevant to Hayhurst. *Id.*, 57-58.

In its Reply, Petitioner argues that Foster is not "limited to streaming 'live' broadcasts" and "also concerns storing secured data." Reply, 26-27. But Patent Owner has never argued that Foster is so limited. Rather, the POR demonstrated that Foster seeks to improve upon prior-art systems (DRMS and CAS) used for live or real-time television/streaming by synchronizing content packets and the keys used to encrypt each. POR, 12-13; *see also* EX1006 [Foster], [0006]-[0007], [0050], [0052].

'116 Paper 29 at 17-18; '854 Sur-Reply, 7

Dr. Bhattacharjee

105. In my opinion, based on my experience and research in this space, I do not agree and POSAs would not agree that there would be "enormous delays" over Foster. *See supra* §VI.B.2 (discussing how Foster-Hayhurst would reduce delays over Foster alone).

106. For one, I note that the '116 patent itself recognizes that sending data via "multiple parallel streams" (as would have occurred in Hayhurst-Foster but not Foster alone) provides for "**increasing speed and efficiency**." EX1001, 70:10-12. Benefits of increased speed and efficiency are **exactly** two of the benefits that I opined would have motivated POSAs to pursue the Foster-Hayhurst combination, which I corroborated with independent prior art (*i.e.*, my opinion was not based on hindsight from the '116 patent's teachings).

'854 EX1111 ¶¶105-106 (cited Reply, 11)
'116 EX1111 ¶¶51-52 (cited Reply, 19-20)

'116 Patent

Similarly, in the case of streaming broadcasts of data (e.g., audio, video), the outgoing data may be parsed and separated into multiple streams each containing a portion of the parsed data. The multiple streams may be transmitted along one or more paths and recombined at the recipient's location in accordance with the present invention. One of the benefits of this approach is that it avoids the relatively large overhead associated with traditional encryption of data followed by transmission of the encrypted data over a single communications channel. The secure parser of the present invention allows data in motion to be sent in multiple parallel streams, increasing speed and efficiency.

'116 EX1001, 70:1-12 (cited Reply, 27)

DEMONSTRATIVE EXHIBIT – NOT EVIDENCE

79

Evidence incorporated-by-reference: Slide 79 contains quotes from the reply declaration at ¶¶ 105-106 that were only cited without explanation in the identified portions of the briefing (-00212 Reply, 19-20; -00215 Reply, 11).

Slide 86:

Foster-Hayhurst: SFI's Argument #4 ("less secure") fails because changing a KEK is not claimed or disclosed by SFI's patents or required by Foster

Dr. Bhattacharjee

106. In my opinion, POSAs would have also disagreed with SFI's argument that the Foster-Hayhurst combination is less secure than Foster's unmodified system. POR, 58-61. That argument is premised on the idea that (**i**) changing or replacing Foster's key-encryption-key ("KEK") would have been more difficult in Foster-Hayhurst because the KEK would have (according to SFI) been located in more than one storage location, and (**ii**) Foster-Hayhurst would have stored the in more locations, which SFI alleges would have made it more vulnerable to attack. POR, 58-61.

107. As to SFI's first allegation regarding the need to update or replace the KEK, I note that the claims do not have any limitations directed to updating or replacing any of the encryption keys, in particular the *external key* that is met by Foster's KEK under SFI's claim constructions. The Foster-Hayhurst combination that I described in my First Declaration did not require updating or replacing the KEK as part of the combination, and thus the combination would not have had to update or replace the KEK. Thus, even if it were true that Foster by itself preferred to have the ability to update / change the KEK, that was not a feature that POSAs would have needed in Foster-Hayhurst for the combination's system to have worked properly, and thus it would not have discouraged POSAs from pursuing the combination. Moreover, the combination had other benefits over Foster alone that would have also motivated the combination (e.g., efficiency, intelligent content delivery, enhanced security from distributed storage, etc.).

108. Furthermore, Foster itself does not **require** updating or replacing the KEK. Instead, Foster explicitly says the KEK "**can** be" (i.e., does not **have** to be) changed in Foster's system. Foster, [0054]. Thus, to the extent SFI is arguing Foster (by itself) required the ability to change its KEK, POSAs would disagree as Foster says otherwise.

109. Foster also recognizes that KEKs "are inherently more secure than title keys, and **do not need to be changed as frequently**." Foster, [0055]. That disclosure in Foster further reinforces my opinion that the ability to change / update the KEK would not have dissuaded POSAs from pursing Foster-Hayhurst because the fact that the KEK did not have to be changed frequently meant it would have been an easier problem to solve compared to an encryption key that had to be changed more frequently.

110. But even though changing and updating the KEK is not required by Foster, Foster-Hayhurst, **or** the challenged claims, POSAs would still disagree with SFI's argument because POSAs would have known how to update and/or replace KEKs that have been distributed across many devices/users. In addition, POSAs would have recognized that whether the encrypted content was stored in one location (as in Foster alone) or across distributed storage devices (as in Foster-Hayhurst), changing the KEK would have to be propagated across the same number of segments. Accordingly, there would be no meaningful difference (let alone insurmountable different requiring more than ordinary skill) to POSAs in complexity between Foster's updating of the KEK and Foster-Hayhurst's updating the KEK. (I note, however, that as I discuss below, Foster-Hayhurst would not have stored the KEK on every storage device in the system anyway.)

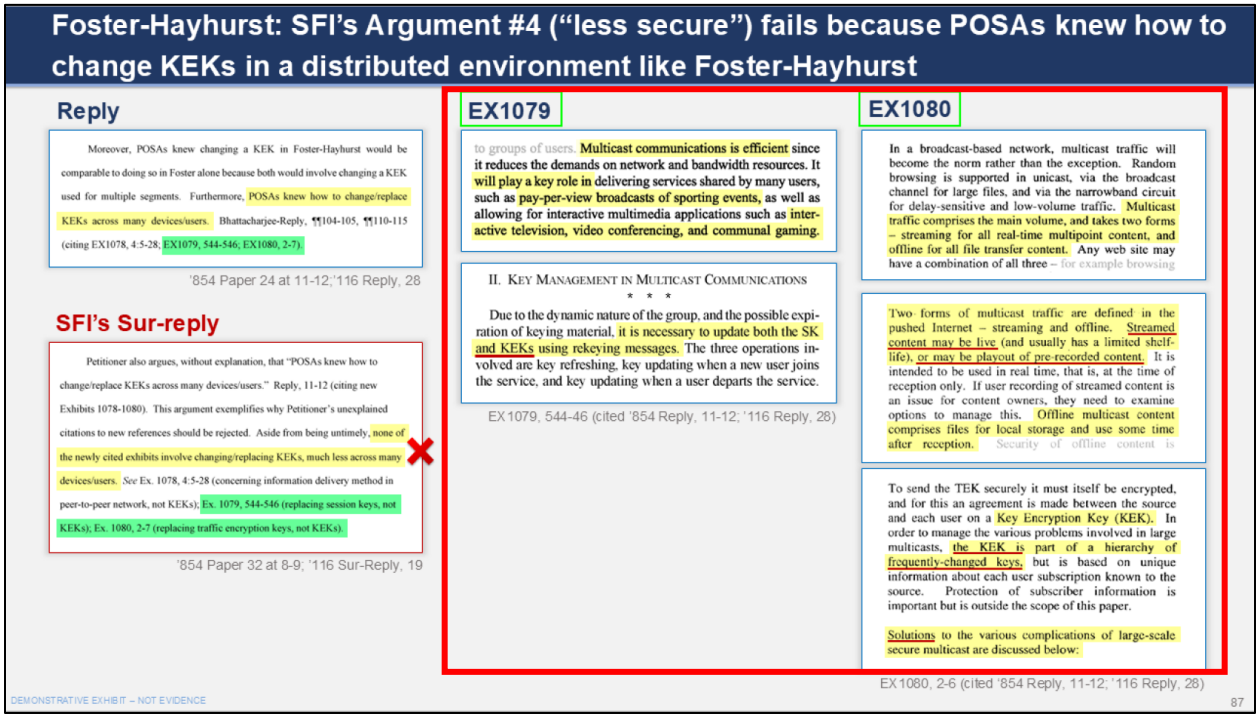
'854 EX1111, ¶¶106-110 (cited Reply, 11)
'116 EX1111, ¶¶159-163 (cited Reply, 28)

DEMONSTRATIVE EXHIBIT – NOT EVIDENCE

86

Evidence incorporated-by-reference: Slide 86 contains quotes from the reply declaration at ¶¶ 106-110 that were only cited without explanation in the identified portions of the briefing (-00212 Reply, 28; -00215 Reply, 11).

Slide 87:



Evidence incorporated-by-reference: Slide 87 contains quotes from Ex. 1079 at 544-546 and Ex. 1080 at 2-6 that were only cited without explanation in the identified portions of the briefing (-00212 Reply, 28; -00215 Reply, 11-12).

Slide 89:

’116/’854 Foster-Hayhurst: SFI’s Sur-Reply argument fails because Foster-Hayhurst has undisputed benefits over Foster alone, and tradeoffs are commonplace

’116 Sur-Reply

Ultimately, “[t]he Board ***must*** weigh the benefits and drawbacks of the modification against each other, to determine whether there would be a motivation to combine.” *Arctic Cat Inc.* v. *Polaris Indus.*, 795 Fed. App’x 827, 833 (Fed. Cir. 2019); POR 56-57, 35 (citing additional cases). But Petitioner does not perform any such weighing in its Reply, and does not dispute Patent Owner’s showing that the numerous drawbacks described in the POR outweigh the benefits alleged in the Petition. *See* Reply, 24-29.

’116 Paper 29 at 20; ’854 Sur-Reply, 10

Reply

But even if Foster-Hayhurst were less secure than Foster in ways SFI alleges (it is not), Foster-Hayhurst added a security technique that Foster lacks (distributed storage) ***and*** provided the other (undisputed) benefits (e.g., speed, intelligence, efficiency, and redundancy) that also motivated Foster-Hayhurst. Petition, 62-63 (citing EX1028-EX1031); Bhattacharjee-Reply, ¶¶174-176 (citing corroboration); *Corephotonics*, 2021 WL 4944471, at *6 (“design decisions entail making tradeoffs among multiple objectives”).

’116 Paper 21 at 29; ’854 Reply, 12

Dr. Bhattacharjee

174. But even if Foster-Hayhurst were less secure than Foster in some of the ways SFI asserts, in my opinion POSAs would have been motivated to pursue Foster-Hayhurst for the reasons I identified in my First Declaration because POSAs would have recognized that the combination would have added various security techniques that Foster lacks, as my First Declaration discussed (and I reiterated above and further below).

175. Separate from improvements in security that I reiterated above, Foster-Hayhurst would have **also** provided other (undisputed) benefits in terms of increased speed, intelligence, efficiency, bandwidth requirements, as I discussed in my First Declaration (¶¶242-246) and above (§VI.B.1). Those benefits would have also motivated POSAs to pursue Foster-Hayhurst, with a reasonable expectation of success. Indeed, POSAs knew that designing an encryption and storage system for encrypted content was a matter of tradeoffs:

> **Data protection** in storage management systems is **a tradeoff** between user’s convenience and security, speed of operation and capabilities of the encryption algorithm, length of the encryption keys, government restrictions, and other elements known in the art. There are many encryption algorithms available that vary by strength, speed and other parameters.

’116 EX1111, ¶¶174-75 (cited Reply, 29); ’854 EX1111, ¶¶121-122 (cited Reply, 12-13)

“[I]t is a commonplace fact that design decisions entail making tradeoffs among multiple objectives. *Allied Erecting and Dismantling Co. v. Genesis Attachments, LLC*, 825 F.3d 1373, 1381 (Fed. Cir. 2016) (‘A given course of action often has simultaneous advantages and disadvantages, and this does not necessarily obviate motivation to combine.’).”

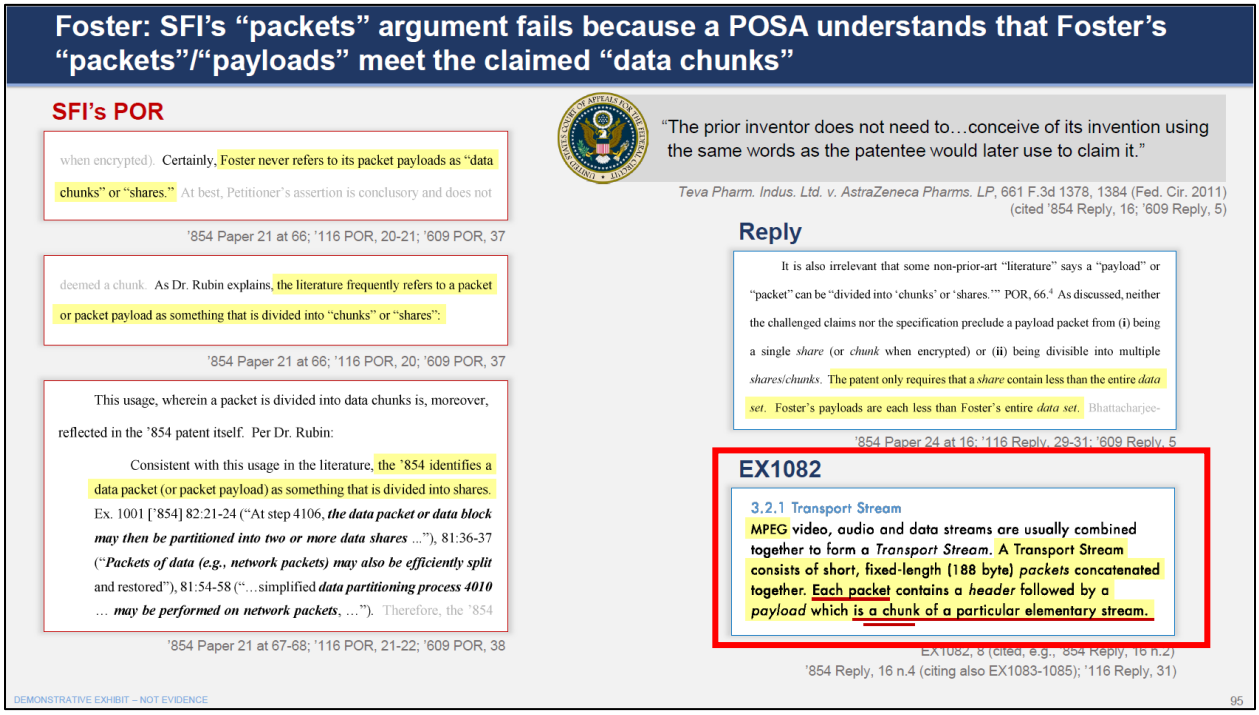
Corephotonics, Ltd. v. Apple Inc., 2021 WL4944471, at *6 (Fed. Cir. Oct. 25, 2021) (cited ’116 Reply, 29; ’854 Reply, 13)

DEMONSTRATIVE EXHIBIT – NOT EVIDENCE

89

Evidence incorporated-by-reference: Slide 89 contains quotes from the reply declaration at ¶¶ 174-175 that were only cited without explanation in the identified portions of the briefing (-00212 Reply, 29; -00215 Reply, 12-13).

Slide 95:



Evidence incorporated-by-reference: Slide 95 contains quotes from Ex. 1082 at 8 that were only cited without explanation in the identified portions of the briefing (-00212 Reply, 31 -00215 Reply, 16 n.4).

Slide 96:

Foster: SFI's "packet" argument also fails because cited literature that SFI ignores says a "packet" can be a "chunk" of a data set

EX1082

3.2.1 Transport Stream

MPEG video, audio and data streams are usually combined together to form a *Transport Stream*. A Transport Stream consists of short, fixed-length (188 byte) *packets* concatenated together. Each packet contains a *header* followed by a *payload* which is a chunk of a particular elementary stream.

EX1082, 8 (cited, e.g., '854 Reply, 16 n.2)

EX1083

A packet is a chuck of data provided by the application program. UDP typically sends a single "application-level packet" as a single UDP packet. However, TCP may break a single application-level packet into multiple smaller TCP "segments", each of which is treated as a separate "packet" at the TCP layer. The Nagle Algorithm (discussed below) does the opposite: It takes multiple small application packets and combines them into a single larger TCP segment.

EX1083, 7:32-40 (cited, e.g., '854 Reply, 16 n.2)

EX1084

[0026] RTP packet: A chunk or portion of multimedia data as sent over an IP network, prepended with certain information, such as a time stamp and a sequence number.

EX1084, [0026] (cited, e.g., '854 Reply, 16 n.2)

EX1085

In one aspect of the invention, there is provided a method for data storage in a distributed data storage system with redundancy, including disassembling a data set into a plurality of data blocks; defining a number of distinct data chunks N; defining a minimal number of data chunks K≦N needed to restore one data block; transforming each of the data blocks into L data chunks, wherein K≦L≦N; and distributing the data chunks to storage elements of the distributed storage system. The storage elements may be different storage for each of data block, or for some of the data blocks. Filler can be added to any data block. Filler can be added to the data set so that the data set is an integral number of data blocks. Each data chunk can include an identifier derived from some function used for its generation. A size of each data chunk can be defined based on an integral number of Message Transfer Units. A size of each data chunk can correspond to packet size, or an integral number of packets. A number L of chunks is chosen such that L≧M+K, where M is maximum number of storage elements that can fail simultaneously.

EX1085, 4:7-25 (cited, e.g., '854 Reply, 16 n.2)

DEMONSTRATIVE EXHIBIT – NOT EVIDENCE

96

Evidence incorporated-by-reference: Slide 96 contains quotes from Ex. 1082 at 8, Ex. 1083 at 7:32-40, Ex. 1084 at [0026], and Ex. 1085 at 4:7-25 that were only cited without explanation in the identified portions of the briefing (-00212 Reply, 31 -00215 Reply, 16 n.4).

Slide 139:

Orsini (Obviousness): POSAs knew encrypting keys with a KEK added additional security beyond what Orsini's obfuscation provides

'609 Reply

Orsini's obfuscation also disregards industry-wide best practices. The National Institute of Standards and Technology ("NIST") advised POSAs that when, as in Orsini, a "key exists external to the cryptomodule, **confidentiality protection shall be provided either by encryption (e.g., key wrapping)** [*i.e.*, a KEK]" or physically protecting keys (like using a safe, which would be inconsistent with Orsini's **electronic** storage of keys). EX1106, 34, 61, 123-125. Bhattacharjee-Reply, ¶¶171-176.

'609 Paper 25 at 26 (citing EX1106, [sic:] 72);* '854 Paper 24 at 19 (citing EX1106)

[12] Because Orsini is electronically storing key information with the data, using physical security (like storing the plain text keys in a safe) is not compatible with Orsini's system (let alone a practical solution for most electronic communication and storage systems).

Dr. Bhattacharjee

176. EX1106 further directs POSAs that the "*confidentiality* of all symmetric and private keys **shall** be protected." EX1106, 72 (all emphasis original). It further states that "[w]hen the symmetric or private key exists external to the cryptomodule, confidentiality protection **shall be provided either by encryption (e.g., key wrapping)** or by controlling access to the key via physical means (e.g. storing the keying material in a safe with limited access)." EX1106, 72 (emphasis of "shall" original).[12] Orsini's method stores the share encryption keys electronically with the data, and so storing the keying material physically in a safe would be contrary to Orsini's system. Thus, EX1106 informs POSAs (as they already knew and consistent with the opinions I offered in my First Declaration), to have "confidentiality protection" of the share keys "provided [] by encryption (e.g., key wrapping)" (i.e., a KEK). EX1106, 72.

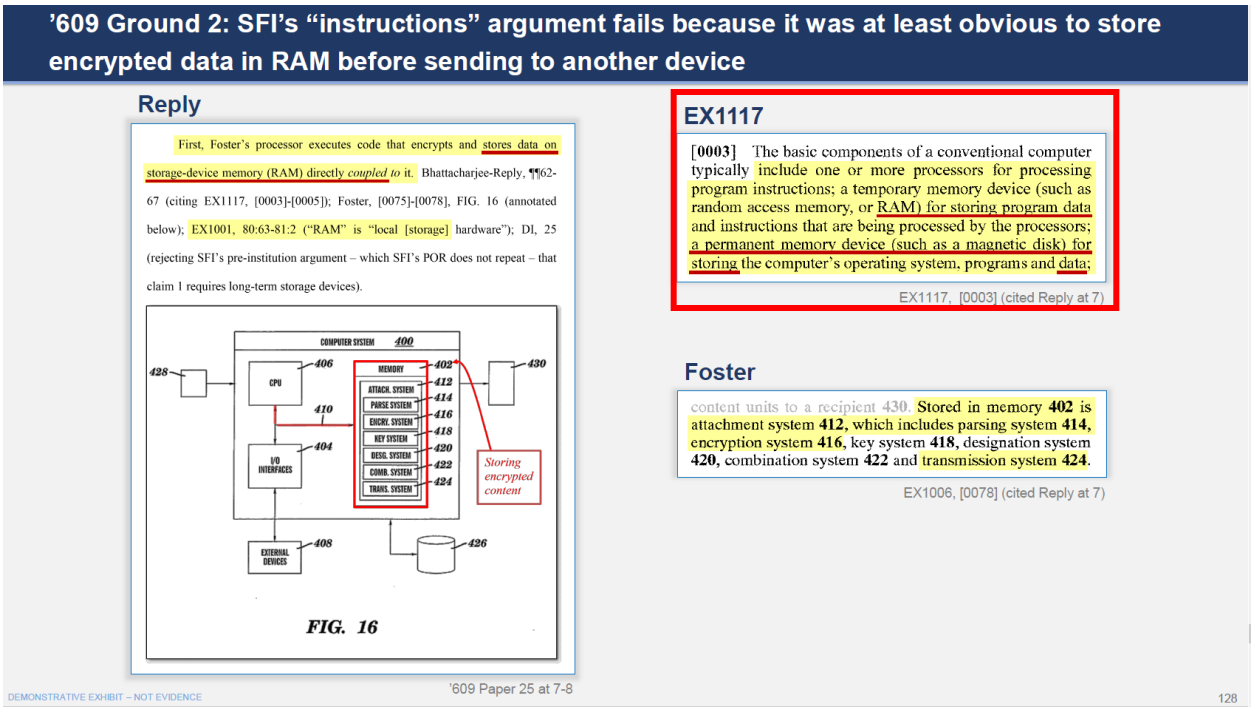
'609 EX1111, ¶176 (cited POR, 26); '854 EX1111, ¶193 (cited POR, 19)

DEMONSTRATIVE EXHIBIT – NOT EVIDENCE

139

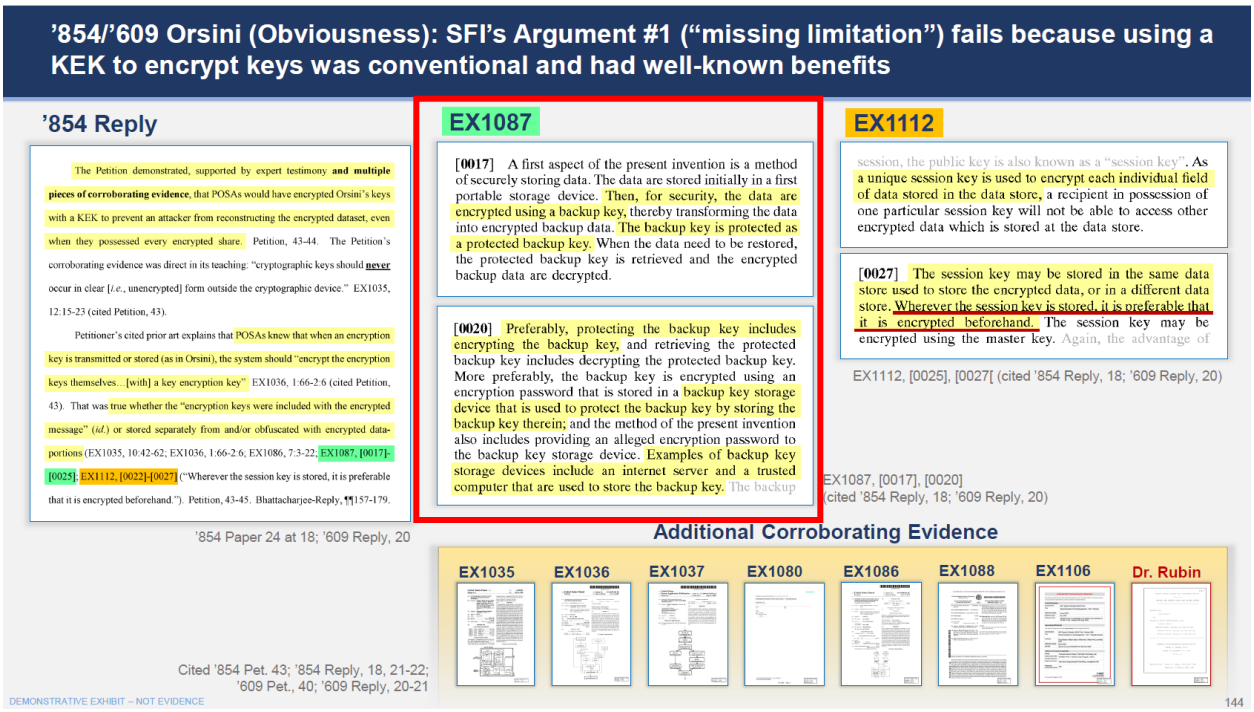
Evidence incorporated-by-reference: Slide 139 contains quotes from the reply declaration at ¶ 176 that were only cited without explanation in the identified portions of the briefing (-00214 Reply, 26; -00215 Reply, 19).

Slide 128:



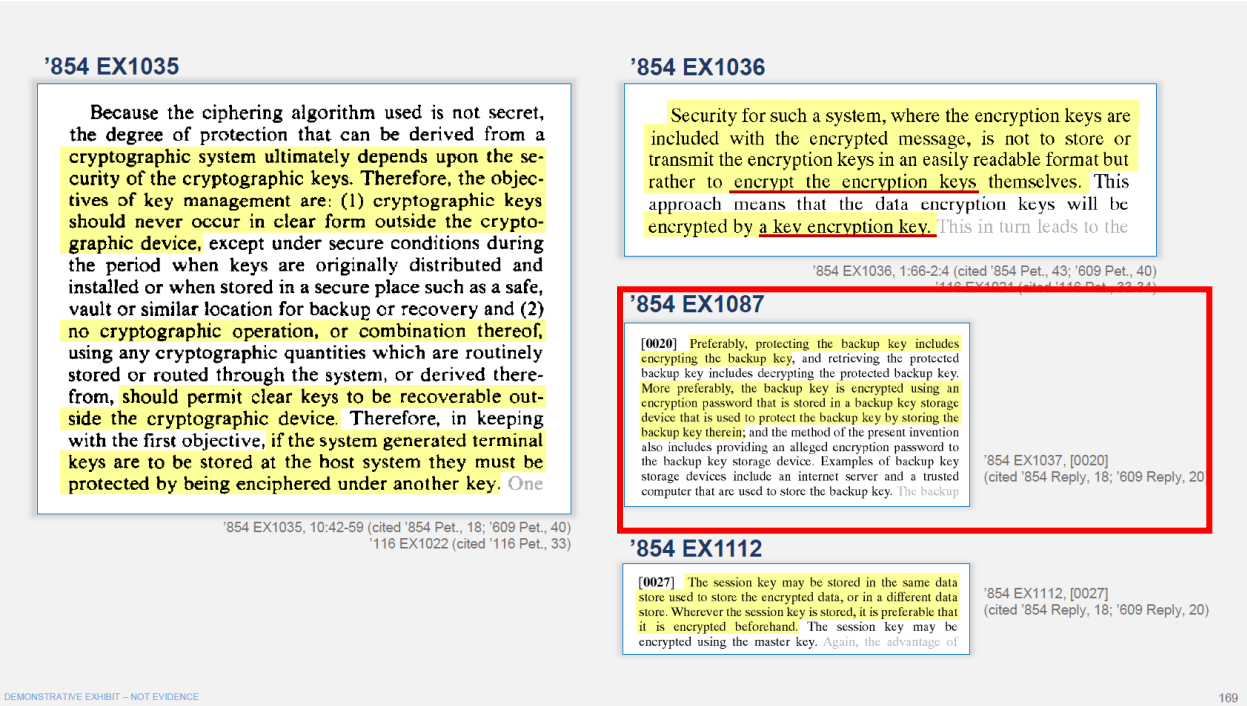
Evidence incorporated-by-reference: Slide 128 contains quotes from Ex. 1117 at [0003] that were only cited without explanation in the identified portions of the briefing (-00214 Reply, 7).

Slide 144:



Evidence incorporated-by-reference: Slide 144 contains Ex. 1087 at [0018], [0020] that was only cited without explanation in the identified portions of the briefing (-00214 Reply, 20; -00215 Reply, 18).

Slide 169:



Evidence incorporated-by-reference: Slide 169 quotes from Ex. 1087 at [0020] that were only cited without explanation in the identified portions of the briefing (-00214 Reply, 20; -00215 Reply, 18).

Respectfully submitted,

/ Stephen J. Elliott /

Stephen J. Elliott (Reg. No. 52,858)
Andrei Iancu (Reg. No. 41,862)
Haley M. Sanders, *pro hac vice*
SULLIVAN & CROMWELL LLP

Kenneth J. Weatherwax (Reg. No. 54,528)
Nathan Lowenstein, *pro hac vice*
Colette Woo, *pro hac vice*
LOWENSTEIN & WEATHERWAX LLP

Date: February 26, 2025

CERTIFICATE OF SERVICE

The undersigned hereby certifies that the following documents were served by electronic service, by agreement between the parties, on the date signed below:

PATENT OWNER'S OBJECTIONS TO PETITIONER'S DEMONSTRATIVE EXHBITS

The names and address of the parties being served are as follows:

Elisabeth H. Hunt	EHunt-PTAB@wolfgreenfield.com
Gregory S. Nieberg	GNieberg-PTAB@wolfgreenfield.com
Nathan R. Speed	nspeed@wolfgreenfield.com

Respectfully submitted,

/ Colette Woo /

Date: February 26, 2025