Trials@uspto.gov
571-272-7822

Paper 15
Entered: December 14, 2015

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

SENSUS USA, INC.,
Petitioner,

v.

CERTIFIED MEASUREMENT, LLC,
Patent Owner.

Case IPR2015-01454
Patent 8,549,310 B2

Before PHILLIP J. KAUFFMAN, BART A. GERSTENBLITH, and PATRICK M. BOUCHER, *Administrative Patent Judges*.

BOUCHER, *Administrative Patent Judge*.

DECISION
Institution of *Inter Partes* Review
37 C.F.R. § 42.108

On June 19, 2015, Sensus USA, Inc. ("Petitioner") filed a Petition pursuant to 35 U.S.C. §§ 311–319 to institute an *inter partes* review of claims 1, 6, and 7 of U.S. Patent No. 8,549,310 B2 ("the '310 patent"). Paper 1. Petitioner filed a Corrected Petition (Paper 4, "Pet.") on July 2, 2015. Certified Measurement, LLC ("Patent Owner") filed a Preliminary

Response (Paper 14, "Prelim. Resp.") on October 1, 2015. Applying the standard set forth in 35 U.S.C. § 314(a), which requires demonstration of a reasonable likelihood that Petitioner would prevail with respect to at least one challenged claim, we institute an *inter partes* review of claims 1, 6, and 7. The Board has not made a final determination of the patentability of any claim.

I. BACKGROUND

A. The '310 Patent

The '310 patent "relates to acquiring and cryptographically certifying a measurement representative of a physical parameter, such that the measurement can be verified at a later time." Ex. 1001, col. 1, ll. 35–38. The "physical parameter" is described broadly as "any physical quantity measurable by a sensor and representable in digital form." *Id.* at col. 4, ll. 39–40. Figure 1 of the '310 patent is reproduced below.

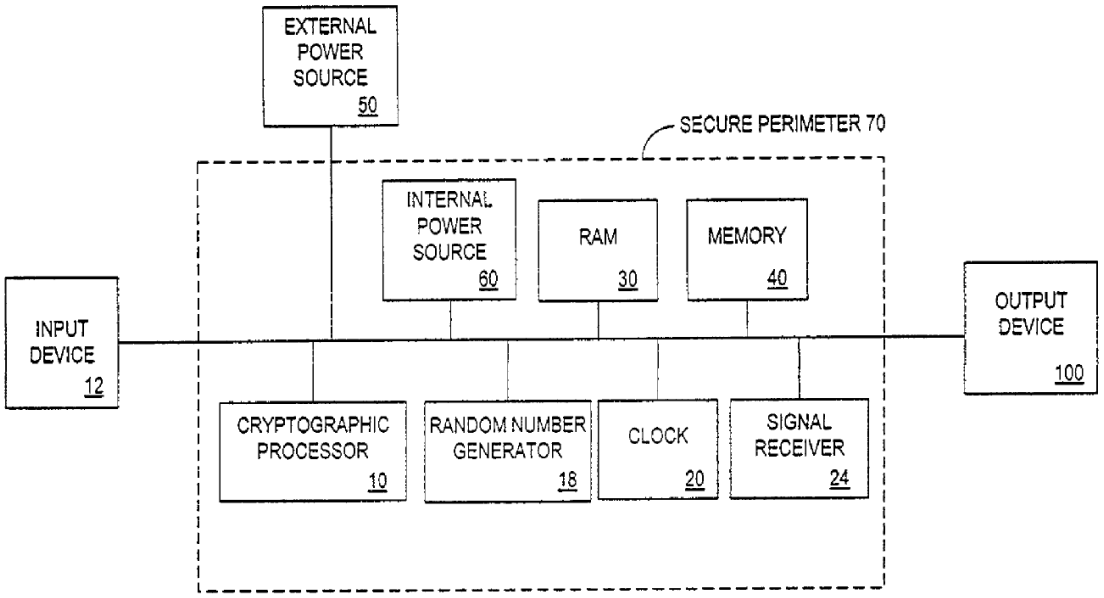

FIG. 1

Figure 1 "illustrates the basic components of a device for secure certification of a physical measurement." *Id.* at col. 6, ll. 66–67. Such basic components are contained within secure perimeter 70, which "may include physical, electronic, or a combination of physical and electronic features to resist tampering." *Id.* at col. 7, ll. 48–58. A measurement taken by a sensor may be certified by adding it to a time from clock 20, creating an "augmented measurement," and then creating a "certified measurement" that comprises the (cleartext) augmented measurement and a (ciphertext) one-way function representative of at least a portion of the augmented measurement. *Id.* at col. 8, ll. 12–27.

B. Illustrative Claim

Claim 1 of the '310 patent is illustrative of the claims at issue:

> 1. A device for secure measurement acquisition and certification, comprising:
>
> (a) a sensor;
>
> (b) a time generator;
>
> (c) a computing device, including a computer processor and a memory, coupled to receive (i) a digital signal being based at least in part on a physical measurement from the sensor and (ii) a second signal being based at least in part on a time from the time generator; said computing device configured for generating an augmented measurement based on the digital signal and the second signal, and for performing a cryptographic operation on at least a portion of the augmented measurement to generate a certified measurement; and
>
> (d) an output device, coupled to the computing device, for writing the certified measurement in response to a certified measurement request;
>
> wherein the sensor, the time generator, and the computing device are configured to be resistant to tampering.

C. References

Petitioner relies on the following references. Pet. 9–10.

Bishop	US 4,077,005	Feb. 28, 1978	Ex. 1005
Cox	US 5,199,068	Mar. 30, 1993	Ex. 1006
Swanson	US 5,689,442	Nov. 18, 1997	Ex. 1007
Blandford	US 5,189,700	Feb. 23, 1993	Ex. 1014
Comerford	US 5,117,457	May 26, 1992	Ex. 1015

Computer Data Authentication, Federal Information Processing Standards Publication 113 (May 30, 1985) (Ex. 1016) ("FIPS113").

D. Asserted Grounds of Unpatentability

Petitioner asserts the following grounds of unpatentability.[1] Pet. 7–8.

Reference(s)	Basis	Claim(s) Challenged
Bishop	§ 102(b)	1, 6, and 7
Cox	§ 102(b)	1, 6, and 7
Swanson	§ 102(e)	1, 6, and 7
Bishop	§ 103(a)	1, 6, and 7
Cox	§ 103(a)	1, 6, and 7
Swanson	§ 103(a)	1, 6, and 7
Cox and Blandford[2]	§ 103(a)	1, 6, and 7

[1] In addition to the grounds identified in the table, Petitioner purports to present challenges under § 103(a) "over Bishop . . . in view of the knowledge of a person of ordinary skill in the art," "over Cox . . . in view of the knowledge of a person of ordinary skill in the art," and "over Swanson . . . in view of the knowledge of a person of ordinary skill in the art." Pet. 7–8. We treat such grounds as subsumed respectively by the asserted grounds under § 103(a) over Bishop alone, Cox alone, and Swanson alone.

[2] Petitioner argues that claim 7 is unpatentable under 35 U.S.C. § 103(a) over Cox and Blandford under two headings, one that combines the argument with its argument directed at claims 1 and 6 (Pet. 37–39), and another that combines its argument with its argument involving FIPS113 (*id.* at 40–43). We do not identify this duplication of its challenges in the table.

Reference(s)	Basis	Claim(s) Challenged
Bishop and Comerford[3]	§ 103(a)	1, 6, and 7
Bishop and FIPS113	§ 103(a)	7
Bishop, FIPS113, and Comerford	§ 103(a)	7
Cox and FIPS113	§ 103(a)	7
Cox, FIPS113, and Blandford	§ 103(a)	7
Swanson and FIPS113	§ 103(a)	7

E. Related Proceedings

The parties assert that the '310 patent is involved in the following litigations: *Certified Measurement, LLC v. CenterPoint Energy Electric Houston, LLC and Itron, Inc.*, 2:14-cv-00627 (E.D. Tex.); *Sensus USA, Inc. v. Certified Measurement, LLC*, 3:14-cv-01069 (D. Conn.); *ALSTOM Grid Inc. v. Certified Measurement, LLC*, 1:15-cv-00072 (D. Del.); and *ABB Inc. v. Certified Measurement, LLC*, 1:15-cv-00461 (D. Del.). Pet. 3–4; Paper 6, 2.

The '310 patent is also the subject of IPR2015-00573, in which an *inter partes* review was instituted on July 9, 2015. *Itron, Inc. v. Certified Measurement, LLC*, Case IPR2015-00573 (PTAB July 9, 2015) (Paper 13). Several petitions have been filed for *inter partes* review of patents related to the '310 patent, as shown in the table below.

[3] Petitioner argues that claim 7 is unpatentable under 35 U.S.C. § 103(a) over Bishop and Comerford under two headings, one that combines the argument with its argument directed at claims 1 and 6 (Pet. 39–40), and another that combines its argument with its argument involving FIPS113 (*id.* at 40–43). We do not identify this duplication of its challenges in the table.

U.S. Patent Challenged	*Inter Partes* Reviews
5,828,751	IPR2015-00570 IPR2015-01262
6,282,648 B1	IPR2015-00571 IPR2015-01311
6,289,453 B1	IPR2015-00572 IPR2015-01439

II. ANALYSIS

A. Claim Construction

The Board interprets claims of an unexpired patent using the broadest reasonable construction in light of the Specification of the patent in which they appear. *See* 37 C.F.R. § 42.100(b); *In re Cuozzo Speed Techs., LLC*, 793 F.3d 1268, 1277–79 (Fed. Cir. 2015); Office Patent Trial Practice Guide, 77 Fed. Reg. 48,756, 48,766 (Aug. 14, 2012).

1. "certified measurement" and "certifiable measurement"

Independent claim 1 recites a "certified measurement" and dependent claim 7 recites a "previously produced certifiable measurement." As Petitioner observes, the term "certifiable measurement" is not recited in the '310 patent Specification outside of its claims, and was added to the claims by amendment during prosecution of U.S. Patent No. 5,828,751, to which the '310 patent claims the benefit of a filing date. Pet. 15–16; Ex. 1001 at [63]; *see Microsoft Corp. v. Multi-Tech Sys. Inc.*, 357 F.3d 1340, 1349–50 (Fed. Cir. 2004) (prosecution history of related application is relevant to claim construction). Patent Owner does not dispute Petitioner's characterization of the related prosecution history as indicating that "Applicant clarified its interpretation of the phrase 'certifiable

measurement,' arguing that the output of the claimed device would not yet be certified." *See* Pet. 15–16.

Petitioner proposes that "certified measurement" be construed as "the result of performing a cryptographic operation on at least a portion of an augmented measurement that . . . has been[] certified," incorporating the explicit language of claim 1, and that "certifiable measurement" be construed as "the result of performing a cryptographic operation on at least a portion of an augmented measurement that is capable of being . . . certified." *Id.* at 16–17 (citing Ex. 1003 ¶ 29). Patent Owner does not proffer proposed constructions of the terms. For purposes of this Decision, we adopt Petitioner's proposed constructions.

2. "cryptographic operation"

Petitioner proposes that "cryptographic operation," which is recited in challenged claims 1 and 6, be construed as "an encryption algorithm or an operation that results in a unique output, based on its input, such that the output is likely to have come from the input and such that the input cannot be readily deduced from the output (excluding algorithms such as CRC)." *Id.* at 18 (citing Ex. 1003 ¶ 33). Patent Owner does not propose an explicit construction of the term.

We do not adopt Petitioner's proposed construction, and instead construe "cryptographic operation" in accordance with its plain and ordinary meaning as an operation that encrypts. Petitioner's proposal to carve out an exception for "algorithms such as [cyclic redundancy check]" is not supported by evidence intrinsic to the '310 patent. As Petitioner recognizes, "[t]he '310 patent does not limit the use of 'cryptographic operation' to any

particular encryption algorithm, and includes the use of one way functions that are not typically considered cryptographic operations." *Id.* at 17 (citing Ex. 1003 ¶ 30; Ex. 1001, col. 4, ll. 48–64, col. 10, ll. 8–14). As such, the '310 patent uses the term "cryptographic operation" expansively, rather than narrowly. Indeed, the patent explicitly states that, under some circumstances, such as "where the primary concern is integrity, a simple one-way algorithm, e.g. . . . cyclic redundancy check (CRC)" might provide an adequate degree of cryptographic processing. Ex. 1001, col. 4, ll. 48–52. We disagree with Petitioner that "the specification then contradicts itself" when it states that "the term one-way function includes . . . cyclic redundancy checks (CRCs), and other techniques well known to those skilled in the art." Pet. 17–18 (citing Ex. 1003 ¶¶ 30–32; Ex. 1001, col. 8, ll. 31–39; Ex. 1013, 3). Indeed, such statements within the '310 patent are internally consistent with a broad construction of "cryptographic operation" that does not exclude "algorithms such as CRC."

We give little weight to the extrinsic evidence cited by Petitioner to support its allegation of inconsistency in the form of an article from *Byte* magazine by one of the named inventors of the '310 patent. *Id.* at 18 (citing Ex. 1013). Although Mr. Schneier suggests a distinction between one-way functions and CRC when he writes in May, 1998, because "it's easy to create a file with a given CRC value," the article was published more than two years after the claimed effective filing date of the '310 patent. In many contexts, such a time lapse is inconsequential, but Mr. Schneier pointedly explains that cryptography differs from other technologies: "It's a situation that most techies aren't used to. . . . [E]ncryption algorithms get easier to

break; something that sufficed three years ago might not today." Ex. 1013, 1.

3. "time"

Neither party proposes a construction of "time." For purposes of this Decision, we adopt the construction adopted for the Institution Decision in IPR2015-00573 for independent claim 1: any chronographic measure, not limited to the time the physical measurement was taken. *Itron v. Certified Measurement*, slip op. at 11.

4. "resistant to tampering"

Independent claim 1 recites that "the sensor, the time generator, and the computing device are configured to be resistant to tampering." Neither party proposes a construction of "resistant to tampering." Consistent with the '310 patent's disclosure that secure perimeter 70 "may include physical, electronic, or a combination of physical and electronic features to resist tampering," we construe the phrase as encompassing physical and/or electronic tamper-resistance mechanisms.

B. Bishop

Bishop relates to a "system for identifying ships and aircraft, both in position and time, utilizing shipboard cryptographic equipment and satellites." Ex. 1005, Abstract. Bishop discloses shipboard "equipment" that stores an individual-identification code word I_S in a storage register, "navigation equipment" that determines a position P of a ship, and a clock that determines the time of day T_1 at which each report is made by the

ship. *Id.* at col. 2, ll. 62–68. Three binary messages corresponding to I_S, P, and T_1 are combined to form a message that Bishop designates as $I_S + P + T_1$, and the combined message is enciphered by a "cryptographic encipherment unit" before transmission by the ship's transmitter. *Id.* at col. 3, ll. 7–14. With respect to independent claim 1, Petitioner draws a correspondence between the recited "sensor" and Bishop's "navigation equipment"; between the recited "time generator" and Bishop's "clock;" between the recited "computing device" and Bishop's "cryptographic encipherment unit"; and between the recited "output device" and Bishop's "transmitter." Pet. 22–26.

Petitioner makes a sufficient showing with respect to these elements. Bishop's "cryptographic encipherment unit" receives a "digital signal being based at least in part on a physical measurement from the sensor" (i.e., based on the determined position P) and receives "a second signal being based at least in part on a time from the time generator" (i.e., based on the time of day T_1). Pet. 24. It also is "configured for generating an augmented measurement" based on those signals (i.e., the combined message $I_S + P + T_1$) and "for performing a cryptographic operation on at least a portion of the augmented measurement to generate a certified measurement" by its encipherment operation. *Id.* at 25.

We are persuaded, at this stage, that the "cryptographic encipherment unit" disclosed by Bishop is "a computing device," as evident from its performance of computational functions in generating and enciphering the combined message. One of skill in the art reasonably would understand such a computing device to include a computer processor and memory. We are not persuaded, at this stage, by Patent Owner's contention that "Bishop's

Figure 1 . . . provides [a] reader no insight whatsoever into its make-up, let alone an indication that it includes a computer processor and a memory." *See* Prelim. Resp. 12–13. As recently reiterated by the Federal Circuit, "a reference can anticipate a claim even if it 'd[oes] not expressly spell out' all the limitations arranged or combined as in the claim, if a person of skill in the art, reading the reference, would 'at once envisage' the claimed arrangement or combination." *Kennametal, Inc. v. Ingersoll Cutting Tool Co.*, 780 F.3d 1376, 1381 (Fed. Cir. 2015) (citing *In re Petering*, 301 F.2d 676, 681 (CCPA 1962)).

1. Anticipation by Bishop

Petitioner contends that claim 1's requirement that "the sensor, the time generator, and the computing device are configured to be resistant to tampering" is disclosed inherently by Bishop. Pet. 26–27 (citing Ex. 1003 ¶ 47; Ex. 1005, col. 1, ll. 36–41, col. 2, ll. 21–30). To establish inherency, the evidence must make clear that the missing descriptive matter is *necessarily present* in the thing described in the reference, and that it would be so recognized by persons of ordinary skill. *In re Robertson*, 169 F.3d 743, 745 (Fed. Cir. 1999). The fact that a certain result or characteristic may occur or be present in the prior art is not sufficient to establish the inherency of that result or characteristic. *In re Rijckaert*, 9 F.3d 1531, 1534 (Fed. Cir. 1993).

Petitioner and Dr. Nielson reason that

> Bishop is directed *primarily* to systems for military ships and aircraft, each of which has its own secure perimeter, and several additional tamper resistant features including without limitation encapsulating computing devices, sensors and clocks where

> they cannot be reached or manipulated while the ship or aircraft is in operation or without special keys or tools, security checkpoints, authorizations and training required to operate or board such ships or aircrafts, etc.

Pet. 26–27 (citing Ex. 1003 ¶ 47) (emphasis added). Petitioner's and Dr. Nielson's inference that Bishop is directed "primarily" to military craft does not exclude the possibility of other implementations. Accordingly, Petitioner does not make a sufficient showing that the tamper-resistance limitation is inherent in Bishop, and, consequently, does not make a sufficient showing to support its anticipation challenge based on Bishop.

We conclude that Petitioner has not demonstrated a reasonable likelihood of prevailing on its challenge of claims 1, 6, and 7 as anticipated by Bishop.

2. Obviousness over Bishop

Petitioner contends that "[t]o the extent such tamper resistant means are not inherently disclosed by Bishop, they would be obvious to a person of ordinary skill in the art." *Id.* at 27 (citing Ex. 1003 ¶ 47). Petitioner cites testimony by Dr. Nielson that such mechanisms "can be as simple as requiring a username and password to access or a case with a lock and key to access the components of the computing device, sensor or clock." Ex. 1003 ¶ 47. Petitioner makes a sufficient showing to support its obviousness challenge against independent claim 1.

Petitioner also makes a sufficient showing for claim 6, which recites that "the cryptographic operation includes encryption with an encryption key," by identifying Bishop's disclosure of the cryptographic encipherment

unit's "use of the current crypto key setting." Pet. 27 (citing Ex. 1003 ¶ 48; Ex. 1005, 3:7–23, col. 3, l. 66–col. 4, l. 3, col. 4, ll. 31–35, col. 4, ll. 47–53).

Claim 7 further recites that "the encryption incorporates a representation of a previously produced certifiable measurement." Petitioner contends that

> a person of ordinary skill in the art would recognize that the disclosed system's ability to perform a cryptographic operation – including encryption – may incorporate a representation of a previously produced certifiable measurement (such as well known, industry standard cipher block chaining methods which are often used when a series of messages is sent, as in Bishop) and that there may be value in transmitting two such measurements in a single message for error checking or where a previous message went undelivered.

Id. at 27–28 (citing Ex. 1003 ¶ 49; Ex. 1016, 4). This contention, repeated by Dr. Nielson, is speculative, and provides insufficient underlying facts or data to support the conclusion. *See* 37 C.F.R. § 42.65(a). As Patent Owner observes, Bishop is explicit in explaining that the cryptographically enciphered message has components I_S, P, and T_1, and that "[n]one of these components is a representation of a previously produced certifiable measurement and Petitioner does not contend or explain otherwise." Prelim. Resp. 18–19.

We conclude that Petitioner has demonstrated a reasonable likelihood of prevailing on its challenge of claims 1 and 6 as unpatentable under 35 U.S.C. § 103(a) over Bishop, but not of prevailing on its challenge of claim 7 on that basis.

3. Obviousness over Bishop and Comerford

Comerford "relates to the provision of physical security for information which is electronically stored." Ex. 1015, col. 1, ll. 11–12. Specifically, Comerford describes "a tamper resistant or intrusion resistant package for protecting information in an electronic circuit" that can detect attempts to tamper with or impair the electronic circuit during an intrusion, to alter the pathways used by the circuitry, or to obliterate or alter stored information. *Id.* at col. 2, l. 44–col. 3, l. 56, col. 7, ll. 3–11, col. 8, ll. 50–65, col. 11, ll. 17–36. Petitioner reasons that "[a] person of ordinary skill in the art would be motivated to combine the communication system of Bishop with the . . . tamper resistant packaging of Comerford in order to heighten security and tamper resistance, which is an inherent goal for costly and dangerous military equipment that Bishop describes." Pet. 40 (citing Ex. 1003 ¶ 77, Ex. 1005, Abstract, col. 1, l. 65–col. 2, l. 10). Patent Owner does not respond to this aspect of Petitioner's argument. Petitioner makes a sufficient showing with respect to claims 1 and 6.

Petitioner's argument related to claim 7, which purports also to present a challenge over Bishop and Comerford, does not explain how Comerford discloses the limitation of claim 7, but instead addresses the teachings of FIPS113. *See id*. at 40–43. Petitioner does not make a sufficient showing with respect to claim 7.

We conclude that Petitioner has demonstrated a reasonable likelihood of prevailing on its challenge of claims 1 and 6 as unpatentable under 35 U.S.C. § 103(a) over Bishop and Comerford, but not of prevailing on its challenge of claim 7 on that basis.

4. Combinations with FIPS113

FIPS113 describes a standard that specifies a data authentication algorithm that "may be used to detect unauthorized modifications, both intentional and accidental, to data." Ex. 1016, 1. Specifically, FIPS113 describes a cipher-block chaining encryption method in which encrypted output O_n is formed by applying an encryption e on a combination of a data block D_n and a previous output O_{n-1}: $O_n = e(D_n + O_{n-1})$. *Id.* at 4. Petitioner reasons that one of ordinary skill in the art would be motivated to apply such cipher-block chaining to the messages of Bishop "to ensure that no messages in the series of messages sent by [that] system[] are lost." Pet. 42 (citing Ex. 1003 ¶¶ 80, 83, 86; Ex. 1016, 4). Petitioner thereby argues that the combination of Bishop, or of Bishop and Comerford, as applied to claims 1 and 6, with this disclosure of FIPS113, would render obvious the additional limitation of claim 7 that "the encryption incorporates a representation of a previously produced certifiable measurement." *Id.* at 42–43. Patent Owner does not respond to this aspect of Petitioner's argument.

We conclude that Petitioner has demonstrated a reasonable likelihood of prevailing on its challenge of claim 7 as unpatentable under 35 U.S.C. § 103(a) over Bishop and FIPS113 and on its challenge of claim 7 as unpatentable over Bishop, Comerford, and FIPS113.

C. Cox

Cox "relates to a system for verifying the identity of [computer-based training system] users who perform the training in an unsupervised environment." Ex. 1006, col. 1, ll. 7–10. When a user registers with the system, a digital copy of the user's signature, along with "discriminator

data" (signature size, signature density ratio, time to create the signature, and potentially the number of erasures) are captured, encrypted, and stored for later use in a verification process. Ex. 1006, col. 4, ll. 3–41. During a subsequent training session, the system randomly generates requests for session signatures, which are registered and stored with the time, date, and discriminator data collected at the time of registration of the session signatures. *Id.* at col. 4, l. 58–col. 5, l. 7. Each of these is then encrypted "for security purposes," and the encrypted data are stored on a magnetic storage medium, enabling subsequent comparison with the original verified signature. *Id.* at col. 5, ll. 35–40, col. 5, l. 52–col. 6, l. 4.

Independent claim 1 recites "a computing device . . . for generating an augmented measurement based on the digital signal and the second signal." Petitioner contends that this limitation is disclosed by Cox because "Cox discloses combining and storing the measured signature, discriminator data (which includes signature size and signature density), and the date and time." Pet. 30 (citing Ex. 1003 ¶ 55; Ex. 1006, col. 1, ll. 49–58, col. 4, l. 67–col. 5, l. 13, col. 5, ll. 35–43, Fig. 2). Petitioner declines to propose a construction for "augmented measurement," contending that the term "is described in the individual claims of the patent." *Id.* at 17. Nevertheless, Petitioner's brief argument suggests a recognition that the formation or production of an "augmented measurement" requires effecting some combination of the physical measurement and time. Such recognition is consistent with the Specification of the '310 patent, which explains that an "augmented measurement" is formed or produced by adding a physical measurement of "any physical parameter or event" to a time, such that the "augmented measurement compris[es] the cleartext time plus the physical

measurement." Ex. 1001, col. 8, ll. 12–22. We disagree that Cox discloses effecting such a combination.

The portions of Cox identified by Petitioner teach that a registered signature is *stored with* a time, but do not disclose combining those data. Petitioner does not explain how the storage of disparate pieces of data, even on the same physical disk, produces or forms an "augmented measurement" as recited in the claims. Dr. Nielson's Declaration, as with its discussion of Bishop, repeats the assertions without providing additional explanation as to how Cox discloses the limitations. *See* 37 C.F.R. § 42.65(a). Petitioner's challenges of dependent claims 6 and 7 suffer from the same deficiency. We conclude that Petitioner has not demonstrated a reasonable likelihood of prevailing on its challenge of claims 1, 6, and 7 as anticipated by Cox.

Petitioner provides no meaningful analysis of its obviousness challenge over Cox independent of its anticipation challenge. Instead, Petitioner relies on a blanket assertion, repeated by Dr. Nielson, that "Cox alone, or in combination with the knowledge of a person of ordinary skill in the art, discloses all of the recitations of the Challenged Claims . . . and either anticipates or renders obvious each such claim." Pet. 28; Ex. 1003 ¶ 50. An "obviousness analysis requires more than an *ipse dixit* assertion that everything in a reference was also well known in the art." *See generally Samsung Elecs. Co. v. Imperium Holdings*, Case IPR2015-01233, slip op. at 18 (PTAB Dec. 1, 2015) (Paper 14). Failure to present evidence of that knowledge and evidence of a rationale for modifying the teachings of the reference in accordance with that knowledge does not comply with 37 C.F.R. §§ 42.104(b)(4) and 42.104(b)(5). We conclude that Petitioner

has not demonstrated a reasonable likelihood of prevailing on its challenge of claims 1, 6, and 7 as unpatentable under 35 U.S.C. § 103(a) over Cox.

We similarly conclude that Petitioner has not demonstrated a reasonable likelihood of prevailing on its remaining challenges based on Cox, i.e., those involving Blandford and/or FIPS113. Those challenges do not resolve Cox's deficiency with respect to "generating an augmented measurement based on the digital signal and the second signal." *See* Pet. 37–39, 39–43.

D. Swanson

Swanson relates "to a surveillance system for capturing and storing information concerning events of interest for subsequent use in investigations and courtroom proceedings." Ex. 1007, col. 1, ll. 6–8. Event sensors controlled by, and connected to, a control processor acquire event information, which is subsequently encrypted and stored. *Id.* at col. 2, l. 58–col. 3, l. 10. To keep track of when certain frames and associated sounds and conditions are acquired, as well as to facilitate subsequent synchronization of information, the control processor maintains a timer and time stamps each frame of event information prior to storage in a data storage device or transmission to a remote location by a transceiver. *Id.* at col. 6, ll. 40–47, col. 10, ll. 43–48. The control processor and data storage device may be installed in an enclosure to protect them "from the environment and from tampering or other harm," including preventing "unauthorized access to the data storage device." *Id.* at col. 11, l. 63–col. 12, l. 4.

Petitioner's analysis setting forth a correspondence between the elements of independent claim 1 and the disclosures of Swanson includes an assertion that "Swanson discloses a device wherein the sensor, time generator, and the computing device are configured to be resistant to tampering." Pet. 35. Petitioner specifically identifies Swanson's disclosure of "protecting the device from tampering by enclosing the device in a temperature controlled enclosure and providing a physical barrier protecting against device damage, tampering and unauthorized access." *Id.* (citing Ex. 1003 ¶ 69; Ex. 1007, col. 11, l. 63–col. 12, l. 4). Dr. Nielson repeats Petitioner's assertions without further analysis. Ex. 1003 ¶ 69.

Independent claim 1 requires that "*the sensor*, the time generator, *and* the computing device are configured to be resistant to tampering" (emphases added). Although the portion of Swanson cited by Petitioner discloses installing the control processor (which includes the timer) and data storage device in an enclosure, it does not address configuring the *sensors* to be resistant to tampering. This is confirmed by an examination of, for example, Figure 1 of Swanson, which shows imaging sensor 12, audio sensor 14, and environment sensor 16 *outside* enclosure 90. Petitioner does not identify adequately disclosure in Swanson of configuring a sensor as recited in the claim to be resistant to tampering. Petitioner's challenges of dependent claims 6 and 7 suffer from the same deficiency.

We conclude that Petitioner has not demonstrated a reasonable likelihood of prevailing on its challenge of claims 1, 6, and 7 as anticipated by Swanson. We also conclude that Petitioner has not demonstrated a reasonable likelihood of prevailing on its challenge of those claims as unpatentable under 35 U.S.C. § 103(a) over Swanson because Petitioner's

conclusory assertion that those claims are unpatentable on that basis lacks sufficient explanation. *See* Pet. 33.

We further conclude that Petitioner has not demonstrated a reasonable likelihood of prevailing on its challenge of claim 7 as unpatentable under 35 U.S.C. § 103(a) over Swanson and FIPS113. Petitioner's reasoning for combining FIPS113 with Swanson does not resolve the deficiency in Petitioner's argument with respect to configuring the sensor to be resistant to tampering. *See id.* at 40–43.

E. Identification of the Real Parties-in-Interest

Petitioner identifies the real parties-in-interest in this proceeding as Sensus USA, Inc., Sensus Worldwide Limited, and Sensus Worldwide Holdings Limited. Pet. 3. Patent Owner contends that this identification is incomplete, and that the Petition should be denied for failing to comply with 35 U.S.C. § 312(a)(2). Prelim. Resp. 29–30. Specifically, Patent Owner provides evidence that, in a related litigation involving the '310 patent,[4] part of the costs of defending the action against Petitioner are covered by insurance. *See* Ex. 2001.

Patent Owner makes the following argument:

> A hallmark of indemnity or insurance agreements that are available to satisfy part or all of a judgment or to reimburse payments of same is an ability for the insurer or indemnitor to control over [*sic*] aspects of the litigation, including the defense and maintenance of an *inter partes* review which seek to invalidate the subject patent.

[4] Patent Owner's reference to "the '648 patent" on page 29 of the Preliminary Response appears intended to refer to the '310 patent.

Prelim. Resp. at 29. Patent Owner's argument is generic and fails to identify any specific evidence that a party other than those identified by Petitioner actually is exercising control over or could exercise control over this proceeding. Patent Owner provides no further analysis of any of the factors identified in *Taylor v. Sturgell*, 553 U.S. 880 (2008), which the Board has confirmed are relevant to an assessment of determining whether an unnamed party constitutes a real party-in-interest. *See Atlanta Gas Light Co. v. Bennett Regulator Guards, Inc.*, Case IPR2013-00453, slip op. at 8–9 (PTAB Jan. 6, 2015) (Paper 88).

Patent Owner asserts that the "Petition should be dismissed for this reason alone, or, alternatively, the Board should authorize immediate discovery on Petitioner's failure to comply with the real party-in-interest requirement." Prelim. Resp. 30. But Patent Owner provides no argument that addresses the *Garmin* factors used by the Board to evaluate whether to authorize additional discovery under 37 C.F.R. § 42.51(b)(2). *See Garmin Int'l, Inc. v. Cuozzo Speed Techs. LLC*, Case IPR2012-00001, slip op. at 6–7 (PTAB Mar. 5, 2013) (Paper 26).

Accordingly, we decline to deny the Petition on this basis or to authorize additional discovery related to the real party-in-interest issue at this time.

III. ORDER

In consideration of the foregoing, it is hereby:

ORDERED that *inter partes* review is *instituted* with respect to the following grounds of unpatentability:

(1) claims 1 and 6 as unpatentable under 35 U.S.C. § 103(a) over Bishop;

(2) claims 1 and 6 as unpatentable under 35 U.S.C. § 103(a) over Bishop and Comerford;

(3) claim 7 as unpatentable under 35 U.S.C. § 103(a) over Bishop and FIPS113; and

(4) claim 7 as unpatentable under 35 U.S.C. § 103(a) over Bishop, Comerford, and FIPS113;

FURTHER ORDERED that *inter partes* review is *not instituted* with respect to any other ground of unpatentability; and

FURTHER ORDERED that pursuant to 35 U.S.C. § 314(a), *inter partes* review of the ’310 patent is hereby instituted commencing on the entry date of this Order, and pursuant to 35 U.S.C. § 314(c) and 37 C.F.R. § 42.4, notice is hereby given of the institution of a trial.

PETITIONER:

Rafael Perez-Pineiro
Javier Sobrado
James A. Gale
FELDMAN GALE, P.A.
rperez@feldmangale.com
JSobrado@FeldmanGale.com
jgale@feldmangale.com

PATENT OWNER:

Tarek Fahmi
Holly Atkinson
ASCENDA LAW GROUP, PC
tarek.fahmi@ascendalaw.com
holly.atkinson@ascendalaw.com