Trials@uspto.gov
571-272-7822

Paper 9
Entered: October 11, 2018

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

AVEPOINT, INC.,
Petitioner,

v.

ONETRUST, LLC,
Patent Owner.

Case PGR2018-00056
Patent 9,691,090 B1

Before BART A. GERSTENBLITH, CARL M. DEFRANCO, and MATTHEW S. MEYERS, *Administrative Patent Judges.*

DEFRANCO, *Administrative Patent Judge*.

DECISION
Institution of Post-Grant Review
35 U.S.C. § 324(a)

OneTrust, LLC ("OneTrust") is the owner of U.S. Patent No. 9,691,090 B1 ("the '090 patent"), which includes twenty-five claims. AvePoint, Inc. ("AvePoint") filed a Petition requesting post-grant review of all twenty-five claims of the '090 patent. Paper 1 ("Pet."). OneTrust filed a Preliminary Response in opposition. Paper 6 ("Prelim. Resp."). Upon

authorization, AvePoint filed a Reply and OneTrust filed a Sur-Reply. Papers 7, 8, respectively. After considering the parties' arguments, as well as all supporting evidence, we determine the Petition shows that more likely than not at least one of the claims of the '090 patent is unpatentable. 35 U.S.C. § 324(a). Thus, we institute post-grant review of claims 1–25 of the '090 patent.

I. BACKGROUND

A. The '090 Patent

The '090 patent issued June 27, 2017, and claims priority to a provisional application filed April 1, 2016.[1] Ex. 1001, 1:10–20. The '090 patent relates to a system and method for assessing a level of risk that a privacy campaign might be compromised. *Id.* at 1:24–29, 2:59–63. A "privacy campaign," according to the '090 patent, includes "any business function, system, . . . , etc., that may utilize personal data collected from one or more persons or entities." *Id.* at 2:53–56. The system uses "servers" and "computing devices" to execute "software modules" that perform "input, processing, storage, retrieval, and display" of data associated with the privacy campaign. *Id.* at 2:48–52.

B. Representative Claim

The '090 patent has two independent claims—method claims 1 and 21—which recite essentially the same steps for calculating the risk level of a privacy campaign, although claim 21 adds the step of "initiating electronic

[1] Because AvePoint filed the Petition within nine months of the '090 patent's issue date and the earliest possible priority date for the '090 patent is after March 16, 2013 (the effective date for the first-inventor-to-file provisions of the Leahy-Smith America Invents Act), the '090 patent is eligible for post-grant review. *See* 35 U.S.C. § 321.

communications to facilitate the input of campaign data by the one or more users." Common across the two independent claims are functional steps of creating an electronic record that utilizes personal data, storing the electronic record, calculating a risk level for the electronic record, and storing the risk level. *See, e.g.*, Ex. 1001, 34:34–35:32. The steps are performed by computer components that include "graphical user interfaces," "storage," and "processors." Claim 1 is representative:

> 1. A computer-implemented data processing method for electronically receiving the input of campaign data related to a privacy campaign and electronically calculating a risk level for the privacy campaign based on the data input, comprising:
>
> displaying on a graphical user interface a prompt to create an electronic record for a privacy campaign, wherein the privacy campaign utilizes personal data collected from at least one or more persons or one or more entities;
>
> receiving a command to create an electronic record for the privacy campaign;
>
> creating an electronic record for the privacy campaign and digitally storing the record;
>
> presenting on one or more graphical user interfaces a plurality of prompts for the input of campaign data related to the privacy campaign;
>
> electronically receiving campaign data input by one or more users, wherein the campaign data comprises each of:
>
> a description of the campaign;
>
> an identification of one or more types of personal data collected as part of the campaign;
>
> at least one subject from which the personal data was collected;
>
> a storage location where the personal data is to be stored; and
>
> data indicating who will have access to the personal data;

processing the campaign data by electronically associating the campaign data with the record for the privacy campaign;

digitally storing the campaign data associated with the record for the campaign;

using one or more computer processors, calculating a risk level for the campaign based on the campaign data and electronically associating the risk level with the record for the campaign, wherein calculating the risk level for the campaign comprises:

electronically retrieving, from a database, the campaign data associated with the record for the campaign;

electronically determining a weighting factor for each of a plurality of risk factors, wherein the plurality of risk factors includes:

a nature of the personal data associated with the campaign;

a physical location of the personal data associated with the campaign;

a number of individuals having access to the personal data associated with the campaign;

a length of time that the personal data associated with the campaign will be retained in storage;

a type of individual from which the personal data associated with the campaign originated; and

a country of residence of at least one subject from which the personal data was collected;

electronically determining a relative risk rating for each of the plurality of risk factors; and

electronically calculating a risk level for the campaign based upon, for each respective one of the plurality of risk factors, the relative risk rating for the respective risk factor and the weighting factor for the risk factor; and

digitally storing the risk level associated with the record for the campaign.

Ex. 1001, 34:34–35:32.

C. The Asserted Grounds of Unpatentability

The Petition asserts that claims 1–25 of the '090 patent are unpatentable as (1) directed to non-statutory subject matter under 35 U.S.C. § 101 (Pet. 28–40); (2) rendered obvious over McQuay,[2] Hunton,[3] Clayton,[4] and Belani[5] under 35 U.S.C. § 103 (*id.* at 40–82); and (3) rendered obvious by AvePoint's prior software product, either alone or in combination with McQuay, Hunton, Clayton, and/or Belani (*id.* at 82–97).

II. ANALYSIS

A. Claim Construction

At this stage, only AvePoint proposes a construction of any particular claim terms, namely, with respect to the steps involved in "calculating a risk level for the campaign." *See* Pet. 24–28. OneTrust believes that "no construction of those terms is necessary at this time" and asks that we "reject [AvePoint's] proposed constructions." Prelim. Resp. 10. Although it criticizes AvePoint's proposed constructions, OneTrust does not offer any of its own. *Id.* at 11–12.

We determine that no express construction of any particular claim term is necessary for purposes of institution. We note, however, that the '090 patent describes the calculation of a "Risk Level" as follows: "Based on weighting factors *and* the relative risk rating for each of the plurality of

---

[2] U.S. Patent No. 8,966,575 B2, iss. Feb. 24, 2015 (Ex. 1005, "McQuay").

[3] Hunton & Williams, CENTER FOR INFORMATION POLICY LEADERSHIP, *The Role of Risk Management in Data Protection*, 31 pp. (Nov. 23, 2014) (Ex. 1008, "Hunton").

[4] U.S. Patent No. 6,904,417 B2, iss. June 7, 2005 (Ex. 1007, "Clayton").

[5] U.S. Patent App. Pub. No. US 2012/0110674 A1, pub. May 3, 2012 (Ex. 1006, "Belani").

factors, the system electronically calculates a risk level for the campaign." Ex. 1001, 4:44–5:1 (emphasis added); *see also id.* at 18:10–67 ("Determining Risk Level").

B. AvePoint's Challenge Under 35 U.S.C. § 101

AvePoint asserts that the claims of the '090 patent do not recite patent eligible subject matter under 35 U.S.C. § 101. Pet. 28–40 (citing Exs. 1001, 1002, 1005–1008, 1018, 1028). OneTrust, in turn, disagrees. Prelim. Resp. 37–55.

The U.S. Supreme Court has long interpreted 35 U.S.C. § 101 to exclude from patenting "[l]aws of nature, natural phenomenon, and abstract ideas." *Alice Corp. Pty. Ltd. v. CLS Bank Int'l*, 134 S. Ct. 2347, 2355 (2014). In determining whether a claim falls within the excluded category of abstract ideas, we are guided by the Supreme Court's two-step framework in *Alice* and *Mayo*. *Id.* at 2356 (citing *Mayo Collaborative Servs. v. Prometheus Labs., Inc.*, 566 U.S. 66, 77–78 (2012)). In accordance with that framework, we first determine whether the claim is "directed to" a patent-ineligible abstract idea. *Id.* ("On their face, the claims before us are drawn to the concept of intermediated settlement, *i.e.*, the use of a third party to mitigate settlement risk."); *see also Bilski v. Kappos*, 561 U.S. 593, 611 (2010) ("Claims 1 and 4 in petitioners' application explain the basic concept of hedging, or protecting against risk.").

If the claim is "directed to" a patent-ineligible abstract idea, we turn to the second step of the *Alice* and *Mayo* framework and consider the elements of the claim, both individually and as an ordered combination, to determine whether the additional elements transform the nature of the claim into a patent-eligible application of the abstract idea. *Alice*, 134 S. Ct. at 2355.

This second step involves a search for an "inventive concept"—an element or combination of elements sufficient to ensure that the claim amounts to "significantly more" than the abstract idea itself. *Id.*

1. Whether the Claims Are Directed to an Abstract Idea

AvePoint asserts that the claims of the '090 patent are directed to nothing more than the abstract idea of assessing the risk of a business's personal data being compromised. Pet. 29; *see also id.* at 31, 34, 35, 37 (repeating same). In support, AvePoint compares the claims of the '090 patent to claims found to be abstract by the U.S. Court of Appeals for the Federal Circuit in *FairWarning IP, LLC v. Iatric Sys., Inc.*, 839 F.3d 1089, 1095 (Fed. Cir. 2016). *Id.* at 31. In that case, the Federal Circuit found the claims to be an abstract idea because they "merely implement an old practice in a new environment," i.e., "the concept of analyzing records of human activity to detect suspicious behavior," while doing so on a computer. *FairWarning*, 839 F.3d at 1093–94 (citing *Alice*, 134 S. Ct. at 2356).

Indeed, the claims here are not unlike the claims found to be an abstract idea in *FairWarning*. More specifically, like the claimed method here, the method in *FairWarning* included the general steps of collecting information regarding computerized transactions and activities associated with personal data, processing and analyzing the information according to one of several rules using certain criterion to determine unauthorized access of the data, and storing the determination for purposes of notifying users. *Id.* at 1093, 1095. While the claims in *FairWarning* recited using one of a few possible rules to analyze the personal data, the Federal Circuit nonetheless found them to be directed to an abstract idea because "the claimed rules ask . . . the same questions (though perhaps phrased with different words) that

humans in analogous situations detecting fraud have asked for decades, if not centuries." *Id.* at 1095. That appears to be the case here.

AvePoint argues that the claims of the '090 patent are directed to an abstract idea because they recite only the "well-known business practice" of risk assessment, albeit implemented on a computer. Pet. 33. According to AvePoint, the steps of "creating" a privacy campaign (i.e., a business function that uses personal data), "assigning" a risk factor/rating to the campaign, and "calculating" a risk level for the campaign can be traced to the "conceptual risk assessment" that businesses have been undertaking "for years." *Id.* (citing Exs. 1001, 1005–1008, 1018). AvePoint's declarant further corroborates this fact, testifying that the recited steps "are underlying principles of any fundamental risk assessment of operations using personal data" and were "part of the state of the art at the time the '090 patent was filed." Ex. 1002 ¶¶ 49–52 (citing Exs. 1005–1011).

OneTrust responds that AvePoint "fails to specifically articulate a single abstract idea recited by the claims" and, even assuming it does, AvePoint "ignores the majority of the claim . . . [and] appears to consider only one claim element." Prelim. Resp. 42–43. We disagree on both counts. AvePoint consistently identifies the abstract idea as assessing the risk of a business's privacy data being compromised. Pet. 29, 31, 34, 35, 37; Ex. 1002 ¶ 52. In addressing directly the limitations of "determining a weighting factor for each of a plurality of risk factors" and "determining a relative risk rating for each of the plurality of risk factors," AvePoint explains that the "concept of taking risk factors and weighing the risk based on how risky each factor is under the circumstances is the underlying principle of any risk assessment." Pet. 29.

In addition to analogizing *FairWarning* to the claims at issue here, AvePoint points to the Federal Circuit's decision in *Electric Power Group, LLC v. Alstom S.A.*, 830 F.3d 1350 (Fed. Cir. 2016). There, the claims were directed to a process for measuring the "vulnerability" of a power grid. *Id.* at 1352. In describing the implementation of the process, "a large portion of the lengthy claims [was] devoted to enumerating types of information and information sources available within the power-grid environment." *Id.* at 1355. Nonetheless, the Federal Circuit held that "merely selecting information, by content or source, for collection, analysis, and display does nothing significant to differentiate a process from ordinary mental processes." *Id.*

Like the claims in *Electric Power*, the claims here are devoted largely to reciting the type of information ordinarily gathered and "known" as relevant to assessing the vulnerability of personal data being compromised. Ex. 1002 ¶ 42; *see also id.* ¶¶ 43–50. As such, we are persuaded at this time that, despite their prolixity, the claims of the '090 patent fail to differentiate meaningfully from ordinary mental processes that humans have been undertaking for years and that Federal Circuit case law has deemed patently ineligible. *See also Content Extraction & Transmission LLC v. Wells Fargo Bank, Nat. Ass'n*, 776 F.3d 1343, 1347 (Fed. Cir. 2014) (finding claims directed to "concept[s] of data collection, recognition, and storage" to be abstract because "humans have always performed these functions").

Nor are we persuaded that the '090 patent discloses a technical improvement to the concept of assessing risk of privacy data being compromised. The specification of the '090 patent supports this notion by describing the key component of the claims—the "processor"—as simply

"one or more general-purpose processing devices such as a microprocessor, a central processing unit, or the like," and, then, providing a laundry list of well-known microprocessors to calculate the risk assessment. Ex. 1001, 11:53–67. That generic description does not amount to an improvement in the way processors operate to calculate risk levels, nor does OneTrust contend as much. *See* Prelim. Resp. 48–50. And, while the '090 patent speaks of an underlying "algorithm" for the processor (*see* Ex. 1001, 4:67–5:7), without more, that ancillary aspect of the calculation does not materially alter the patent eligibility of the abstract idea. *See Elec. Power Grp.*, 830 F.3d at 1354 (finding "analyzing information by steps people go through in their minds, or by mathematical algorithms, without more, as essentially mental processes within the abstract-idea category") (citations omitted). In sum, we are persuaded that the evidence of record, as well as the case law, supports finding that the independent claims of the '090 patent are directed to an abstract idea that lacks any technical improvement.

2. Whether the Claims Include an Inventive Concept

Moving to the second step of the *Alice* and *Mayo* framework, we consider the limitations of the claims "individually and 'as an ordered combination'" to determine whether any additional elements "'transform the nature of the claim into a patent-eligible application" of the claimed concept. *Alice*, 134 S. Ct. at 2355 (quoting *Mayo*, 566 U.S. at 78, 79). In other words, we are looking to see if the claims have "something more" that would transform them from an abstract idea into an *inventive* concept. *Alice*, 134 S. Ct. at 2354.

AvePoint urges that the independent claims recite nothing more than an abstract idea because they include only "conventional and functional

components incidental to implementing the abstract idea of assessing the risk of a business operation that uses personal data." Pet. 35. OneTrust responds that AvePoint "fails to provide any evidence" that the claims recite only routine and conventional activity. Prelim. Resp. 51; *see also id.* at 48–49 ("the Petition fails to point to any evidence suggesting that . . . the components were conventional"). On the current record, we find that AvePoint proffers sufficient proof that the claims recite nothing more than routine and conventional activity for implementing the abstract idea of assessing the risk level of a privacy campaign.

In particular, the current record reflects that the claims of the '090 patent simply add conventional computer components—"graphical user interface," "storage," and "processors"—to the well-known practice of evaluating and determining risk levels for personal data used in a business environment. None of those components, as described and claimed in the '090 patent, is limited or specialized in any meaningful way. *See, e.g.*, Ex. 1001, 2:64–3:4, 3:64–4:2 (describing graphical user interface), 3:18–21, 10:9–11 (describing storage devices), 11:53–67 (describing processors).

Nor are the claimed "risk factors" outside the norm of what would typically underlie a risk assessment of personal data being compromised. In asserting that the claimed risk factors were "well-known to those of skill in the art" and merely a matter of "common sense" (Pet. 36–37), AvePoint relies on the testimony of its declarant, who cites numerous contemporaneous documents showing the routine and conventional nature of the claimed risk factors. *See* Ex. 1002 ¶¶ 42–50 (citing Exs. 1005–1011). In particular, AvePoint's declarant testifies that the recited "risk factors" were "well known in the art" of safeguarding "medical information, financial

information, such as credit card numbers, or non-public personal identifying information, such as social security numbers." *Id.* ¶ 43. That testimony, which is unrebutted at this stage, speaks to the conventional wisdom in the industry of data protection. Thus, without more, we discern no reason to doubt its credibility.

Moreover, the testimony of AvePoint's declarant is consistent with the acknowledgement in the "Background" section of the '090 patent itself that the claimed risk factors were a common aspect of existing "data protection risk assessments" and "privacy audits" performed by "many companies handling personal data," such as Google and Facebook. Ex. 1001, 2:9–39. Specifically, the factors considered by those companies in assessing the risk of a privacy breach included "where personal data comes from, where it is stored, who is using it, where it has been transferred, and for what purpose is it being used." *Id.* at 2:29–34. Those known factors are essentially no different than the "risk factors" recited in the independent claims—"type of individual from which the personal data . . . originated," "physical location of the personal data," "individuals having access to the personal data," "subject[s] from which the personal data was collected," and "nature of the personal data." *Id.* at 35:10–23. Thus, we find that the '090 patent itself, in describing the existing knowledge in the art, serves as further proof of the routine and conventional nature of the claimed method.

Aside from that factual evidence, AvePoint cites several Federal Circuit decisions to show that the claims must add more than mere "token steps," such as ancillary pre- or post-solution activity, insignificant data-gathering steps, or the like, to elevate the claims beyond the recited abstract idea. Pet. 30 (citing *OIP Techs., Inc. v. Amazon.com, Inc.*, 788 F.3d 1359,

1362–63 (Fed. Cir. 2015) ("At best, the claims describe the automation of the fundamental economic concept of offer-based price optimization through the use of generic-computer functions . . . [b]ut relying on a computer to perform routine tasks more quickly or more accurately is insufficient to render a claim patent-eligible."); *Ultramercial, Inc. v. Hulu, LLC*, 772 F.3d 709, 716 (Fed. Cir. 2014) ("the steps of consulting and updating an activity log represent insignificant 'data-gathering steps'")); *see also Accenture Global Servs. v. Guidewire Software, Inc.*, 728 F.3d 1336, 1345 (Fed. Cir 2013) (finding limitations directed to "essentially a database of tasks, a means to allow a client to access those tasks, and a set of rules that are applied to that task . . . do not provide sufficient additional features or limit the abstract concept in a meaningful way"). We are persuaded that, like the claims in those seminal cases, the claims here do not add meaningful limitations beyond the recited abstract idea, and in practical effect, preempt the abstract idea. Thus, in addition to factual evidence, AvePoint explains through case law comparison why the claims lack inventive concept. OneTrust makes no attempt to distinguish the case law relied upon by AvePoint. *See* Prelim. Resp. 50–53.

3. Conclusion

After considering the evidence and arguments presented in the Petition and Preliminary Response, we determine that AvePoint more likely than not will prevail in showing that at least one of the challenged claims is

unpatentable under 35 U.S.C. § 101. As such, we institute post-grant review of all the challenged claims.[6] *See* 35 U.S.C. § 324(a).

C. AvePoint's Additional Challenges Under 35 U.S.C. § 103

1. Obviousness Over McQuay, Hunton, Clayton, and Belani

AvePoint argues that claims 1–25 are also unpatentable as obvious over the prior art references of McQuay, Hunton, Clayton, and Belani. Pet. 40–82. Notably absent from AvePoint's Petition, however, is any articulation of a reason to combine the teachings of these references, a critical factor in considering obviousness. *See id.* Nor do we discern that AvePoint's declarant compensates for this failure, for he testifies only as to the state of the art and the level of skill in the art, but never addresses a reason to combine the art. *See* Ex. 1002 ¶¶ 30–51. During trial, AvePoint will have an opportunity to convince us otherwise. Nonetheless, because

[6] OneTrust contends that section 101 is "not available as a ground to cancel a claim in a PGR" because only sections 102 and 103 are a "condition for patentability" as used in section 282 of the patent statute. Prelim. Resp. 54–55. We disagree. The Supreme Court characterizes patent eligibility under section 101 as a "threshold test" for patentability. *Bilski v. Kappos,* 561 U.S. 593, 602 (2010). And the Federal Circuit has long held that "the Patent Act sets out the conditions for patentability in three sections: sections 101, 102, and 103." *Aristocrat Techs. Austl. PTY Ltd. v. Int'l Game Tech.*, 543 F.3d 657, 661–62 (Fed. Cir. 2008) (citing *Graham v. John Deere Co. of Kansas City*, 383 U.S. 1, 12 (1966)). To the extent OneTrust relies for support on the title "Conditions for patentability" in sections 102 and 103, we are not persuaded. "The title of a statute . . . cannot limit the plain meaning of the text. For interpretive purposes, it is of use only when it sheds light on some ambiguous word or phrase." *Pa. Dep't of Corrs. v. Yeskey*, 524 U.S. 206, 212 (1998) (quoting *Trainmen v. Baltimore & Ohio R.R. Co.*, 331 U.S. 519, 528–529 (1947)). Here, the text of section 101 plainly reads as a fundamental precondition to obtaining a patent—if you invent something "new and useful," then you "may obtain a patent therefor."

"[e]qual treatment of claims and grounds for institution purposes has pervasive support in [*SAS Institute Inc. v. Iancu*, 138 S. Ct. 1348 (2018)]," we institute post-grant review of this obviousness ground as set forth in the Petition. *PGS Geophysical AS v. Iancu*, 891 F.3d 1354, 1360 (Fed. Cir. 2018); *see also Adidas AG v. Nike, Inc.*, 894 F.3d 1256, 1258 (Fed. Cir. 2018) (remanding for Board to consider non-instituted ground).

2. Obviousness Over AvePoint's Prior Use, Alone or in Combination with McQuay, Hunton, Clayton, and/or Belani

AvePoint argues that claims 1–25 are also unpatentable as obvious over AvePoint's prior public use of a software program called "AvePoint Privacy Impact Assessment (APIA)." Pet. 82–97. Pointing to press releases and a Google analytics report, AvePoint asserts that, by May 2014, the APIA software product was "downloaded by more than 1,200 people in 62 countries" well before the April 2016 effective filing date of the '090 patent. *Id.* at 83 (citing Exs. 1020–22). One of the press releases mentions "live demonstrations" of the APIA software at a global conference held in March 2014, where attendees were invited to "AvePoint's booth" to participate in "one-on-one discussions" about the APIA software. Ex. 1020, 2. As evidence of the software's operation, AvePoint proffers a "User Guide" and contemporaneous screenshots disclosing or suggesting each of the claim elements. Pet. 84–92 (citing Exs. 1023, 1024). And, to corroborate that the APIA software features described in the User Guide and screenshots were available to the public "as early as February 2014," AvePoint submits the declaration of one of the presenters at the March 2014 global conference. Ex. 1029 ¶¶ 3, 11.

OneTrust raises several arguments in response to AvePoint's purported prior public use of the APIA software, including (1) "the software

itself is totally absent from the record," (2) the petition "fails to present any evidence of actual prior public use of that software," and (3) there is "no evidence that the [software] system was actually used to perform each and every method step." Prelim. Resp. 63–64; *see also* Sur-Reply 3. As to OneTrust's first and second points, we are not persuaded, for the Petition presents ample documentary and testimonial evidence describing the APIA software's use and operation, as well as the public nature of such use before the critical date in this case. *See* Exs. 1020–1027, 1029. At this stage, we have no reason to believe that this evidence is inaccurate or untrustworthy. Certainly nothing on the face of the documents suggests as much. And the testimony, made under oath, appears credible and consistent with statements in the documents. In any event, during trial, OneTrust is free to test and investigate the evidence relied upon by AvePoint and introduce rebuttal evidence.

As for the third point raised by OneTrust—that the Petition "completely ignores entire claim elements" in asserting that the February 2015 version of the APIA software performed the claimed method (Prelim. Resp. 71–73), we disagree. AvePoint submits a detailed claim chart mapping *each element* of the claims to the APIA software's User Guide and/or screenshots, all of which are dated on or before February 2015. Pet. 84–92 (citing Exs. 1023, 1024). As for the particular claim elements OneTrust accuses AvePoint of ignoring, we note that AvePoint provides pinpoint citations of their disclosure in the User Guide and screenshots. *See, e.g.*, Pet. 87 (citing Ex. 1023, 16, 40, for the step of "electronically . . . associating campaign data with the privacy campaign"); *id.* at 86 (citing Ex. 1023, 36–38, for the step of "creating an electronic record . . . and

digitally storing . . . the record"); *id.* at 86–87 (citing Ex. 1023, 13–15, 25, with respect to the step reciting "wherein the campaign data comprises . . ."). Thus, we are not persuaded that the Petition fails to demonstrate how the APAI software performed each of the claimed steps.

All said, however, we do agree with OneTrust that, to the extent AvePoint asserts a ground that relies on the APIA software "in combination with McQuay-Hunton-Clayton-Belani," we again note the absence of any reason to combine in the Petition (as well as the supporting declaration). Pet. 84; *see also id.* at 97 (similarly lacking in explanation). Thus, as with the previous ground, AvePoint will have an opportunity to convince us otherwise during trial. Nonetheless, we institute trial on the APIA software-based grounds as raised in the Petition. *See PGS Geophysical*, 891 F.3d at 1360 ("[e]qual treatment of claims and grounds for institution purposes has pervasive support in *SAS*").

D. 35 U.S.C. § 325(d)

OneTrust argues that the Petition should be dismissed under 35 U.S.C. § 325(d) because it "simply reiterates the Examiner's rejection under 35 U.S.C. § 101 during prosecution" of the '090 patent. Prelim. Resp. 37–41; *see also* Sur-Reply 1. We disagree. The Examiner did not have the benefit of evidence showing that the claimed "risk factors," identified as the reason for allowance (*see* Ex. 1004, 191), were routine and conventional aspects of any data protection risk assessment, as discussed above. Thus, we do not believe the particular circumstances of this case warrant invoking our discretion under 35 U.S.C. § 325(d).

III. ORDER

Accordingly, it is hereby:

ORDERED that, pursuant to 35 U.S.C. § 324(a), a post-grant review of claims 1–25 of the '090 patent according to the grounds raised in the petition is hereby *instituted*; and

FURTHER ORDERED that, pursuant to 35 U.S.C. § 324(d) and 37 C.F.R. § 42.4(b), a post grant review of the '090 patent will commence on the entry date of this Order, and notice is hereby given of the institution of a trial.

FOR PETITIONER:

Nathan A. Evans
Michele Mayberry
WOODS ROGERS PLC
nevans@woodsrogers.com

FOR PATENT OWNER:

David A. Reed
Michael T. Morlock
KILPATRICK TOWNSEND & STOCKTON LLP
dreed@kilpatricktownsend.com
mmorlock@kilpatricktownsend.com

Scott E. Brient
BRIENT IP LAW, LLC
sbrient@brientip.com

David K. Dabbiere
ONETRUST, LLC
ddabbiere@onetrust.com