Trials@uspto.gov
571-272-7822

Paper 46
Date: October 10, 2019

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

AVEPOINT, INC.,
Petitioner,

v.

ONETRUST, LLC,
Patent Owner.

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*.

JUDGMENT
Final Written Decision
Determining All Challenged Claims Unpatentable
35 U.S.C. § 328(a)

OneTrust, LLC is the owner of U.S. Patent No. 9,691,090 B1, which includes twenty-five claims. Ex. 1001 ("the '090 patent"). AvePoint, Inc. filed a petition for post-grant review of all twenty-five claims of the '090 patent. Paper 1 ("Pet."). We instituted post-grant review of all claims

as challenged in the Petition. Paper 9 ("Inst. Dec."). OneTrust filed a Patent Owner Response. Paper 20 ("PO Resp."). AvePoint filed a Reply. Paper 24 ("Pet. Reply"). And OneTrust filed a Sur-Reply. Paper 30 ("Sur-Reply"). In addition, OneTrust moved to strike a purportedly "new" expert declaration submitted with AvePoint's Reply. Paper 27 ("Mot. To Strike"). And AvePoint followed with its own motion to exclude the declaration of OneTrust's expert. Paper 34 ("Mot. to Exclude").

We have jurisdiction under 35 U.S.C. § 6. An oral hearing was conducted on June 28, 2019. Paper 45 ("Tr."). After considering the parties' arguments and supporting evidence, we determine that AvePoint has proven, by a preponderance of the evidence, that claims 1–25 of the '090 patent are unpatentable. 35 U.S.C. § 326(e). Also, we deny OneTrust's motion to strike and AvePoint's motion to exclude.

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, codes (45), (60), 1:10–20. The '090 patent describes "a data processing system and method . . . for electronically receiving the input of campaign data associated with a privacy campaign, and electronically calculating a risk level for the privacy campaign based on the campaign data." *Id.* at 2:59–63; *see also id.* at 1:24–

[1] The '090 patent is eligible for post-grant review because AvePoint filed its Petition within nine months from the '090 patent's issue date, and the earliest possible priority date of 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). *See* 35 U.S.C. § 321. OneTrust does not contest the eligibility of the '090 patent for post-grant review.

29 (describing essentially same). According to the '090 patent, a "privacy campaign may be any business function, system, product, technology, process, project, engagement, initiative, campaign, etc., that may utilize personal data collected from one or more persons or entities." *Id.* at 2:53–56.

The "Background" section of the '090 patent explains that certain regulations in the United States, Canada, and the European Union require companies to conduct privacy impact assessments or data protection risk assessments. *Id.* at 1:62–2:9. "For many companies handling personal data," these risk assessments "are not just a best practice, they are a requirement . . . to ensure that their treatment of personal data comports with the expectations of [regulators]." *Id.* at 2:21–29. The '090 patent identifies "Facebook and Google," in particular, as being required to show that their data protection risk assessments comply with federal privacy regulations. *Id.*

With that in mind, the '090 patent provides "a system for operationalizing privacy compliance." *Id.* at 2:46–47. As described, the system is comprised of "servers and client computing devices that execute one or more software modules that perform functions and methods related to *the input, processing, storage, retrieval, and display of campaign data* related to a privacy campaign." *Id.* at 2:48–52 (emphasis added). "The system presents on one or more graphical user interfaces a plurality of prompts for the input of campaign data related to the privacy campaign." *Id.* at 3:1–4. Then, "[u]sing a microprocessor, the system calculates a 'Risk Level' for the campaign based on the campaign data, . . . and digitally stores the risk level." *Id.* at 3:2–21. The system calculates the risk level based on

risk factors, which the background of the '090 patent lists as "where personal data comes from, where is it stored, who is using it, where it has been transferred, and for what purpose is it being used." *Id.* at 2:29–34. A "weighting factor" and a "relative risk rating" are assigned to each of those factors. *Id.* at 4:44–64. "Based on weighting factors and the relative risk rating for each of the plurality of [risk] factors," the system "may use an algorithm" to calculate the risk level, for example,

> as the sum of a plurality of: a weighting factor multiplied by the relative risk rating of the factor (i.e., Risk Level for campaign = (Weighting Factor of Factor 1) * (Relative Risk Rating of Factor 1) + (Weighting Factor of Factor 2) * (Relative Risk Rating of Factor 2) + . . . (Weighting Factor of Factor N) * (Relative Risk Rating of Factor N).

Id. at 4:64–5:7.

B. The Challenged Claims

The '090 patent has two independent claims—method claims 1 and 21—which recite essentially the same steps for calculating a risk level for a privacy campaign.[2] Claim 1 is representative and recites:

> 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;

[2] Claim 21 merely adds the step of "initiating electronic communications to facilitate the input of campaign data by the one or more users."

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 (emphases added).

C. The Asserted Grounds of Unpatentability

AvePoint asserts the following grounds in challenging the patentability of claims 1–25 (Pet. 13–14):

Challenged Claims	35 U.S.C.	Basis
1–25	§ 101	
1–25	§ 103	McQuay,[3] Hunton,[4] Clayton,[5] and Belani[6]

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

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

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

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

1–25	§ 103	AvePoint's Software Product[7] alone or in combination with McQuay, Hunton, Clayton, and/or Belani

II. ANALYSIS

A. Claim Construction

We give claim terms in an unexpired patent their broadest reasonable interpretation in light of the specification of the patent in which they appear. 37 C.F.R. § 42.200(b) (2017). Here, AvePoint proposes a construction for the claimed steps of "determining a weighting factor," "determining a relative risk rating," and "calculating a risk level." Pet. 24–28. According to AvePoint, the combination of those steps means

> *each risk factor is given a relative risk rating* based on known risk associated with that factor, *a weight is given to each risk factor* based on known risk associated with that factor, and the only calculation described is an algorithm multiplies the relative risk rating by the weighting factor to obtain a value for each risk factor that indicates the security risk for that attribute of personal data, then the algorithm adds together all the values for the risk factors to calculate an overall risk level for the campaign.

Id. at 28 (emphases added).

OneTrust responds that AvePoint's proposed construction "conflates the two steps into one," and "reads out the requirement of separate 'weighting factors' and 'relative risk ratings'" for each of the respective risk factors. PO Resp. 31–32. As such, OneTrust asserts that we "should give the claim language its plain and ordinary meaning, which requires a separate 'weighting factor' and 'relative risk rating' for each respective risk factor." *Id.* at 34.

[7] AVEPOINT PRIVACY IMPACT ASSESSMENT USER GUIDE (Ex. 1023).

We do not view AvePoint's proposed construction in the manner OneTrust would have us. In our view, AvePoint makes clear in the Petition that "*[e]ach particular risk factor* is assigned a weighting factor . . . as well as a risk rating." Pet. 24; *see also id.* at 28 ("each risk factor is given a relative risk rating . . . a weight is given to each risk factor"). Indeed, AvePoint points expressly to the '090 patent's description of the weighting factor being multiplied by the risk rating to produce a single value *for each risk factor*. *Id.* at 25 (citing Ex. 1001, 5:1–7). Those assertions show that AvePoint fully recognizes the distinction in assigning both a "weighting factor" and a "risk rating" to each risk factor in the calculation of a risk level. In any event, AvePoint subsequently made clear in its Reply that it agrees with OneTrust's proposed construction. Pet. Reply 4–5. Thus, we adopt OneTrust's construction that the claim language "requires a separate 'weighting factor' and 'relative risk rating' for each respective risk factor." PO Resp. 31, 34; *see also* Ex. 1001, 4:59–5:15, 20:30–35 (supporting that the claimed "weighting factor" and "relative risk rating" are distinct "numerical" values).

That said, however, we reject any attempt by OneTrust to limit the meaning of the claimed "weighting factor" and "relative risk rating" to values that are only "customizable." PO Resp. 34 (citing Ex. 1001, 18:58–67, 20:10–55). Neither the claim language nor the Specification support such a narrow construction. Indeed, the Specification provides expressly that the weighting factor may encompass "default settings . . . *or* customizations." Ex. 1001, 20:13–16 (emphasis added). Likewise, as described, the relative risk rating may encompass either "default values . . . *or* . . . customized values." *Id.* at 20:26–28 (emphasis added); *see also id.* at

20:47–50 ("the privacy campaign may be assigned based on the following criteria, which may be either a default *or* customized setting") (emphasis added). In both instances, the default values are "based on privacy laws." *Id.* at 20:13–50. Thus, when properly construed in light of the Specification, the weighting factor and relative risk rating may include customizable values *or* pre-assigned default values.

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

AvePoint asserts that the challenged claims do not recite patent eligible subject matter under 35 U.S.C. § 101. Pet. 28–40. OneTrust disagrees. PO Resp. 69–93. Section 101 of the patent statute defines patent-eligible subject matter as "any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof." 35 U.S.C. § 101. Laws of nature, natural phenomenon, and abstract ideas, however, are not patentable. *Alice Corp. v. CLS Bank Int'l*, 573 U.S. 208, 217 (2014) ("*Alice*") (citing *Mayo Collaborative Servs. v. Prometheus Labs., Inc.*, 566 U.S. 66, 77–78 (2012) ("*Mayo*"), and *Bilski v. Kappos*, 561 U.S. 593, 601–02 (2010) ("*Bilski*")). Here, AvePoint relies on the judicial exception of abstract ideas to argue that the challenged claims are patent ineligible. Pet. 28–40; Pet. Reply 8–18.

In evaluating whether the challenged claims are "directed to" an abstract idea, we are guided by the framework set forth in *Alice* and *Mayo*. *Alice*, 573 U.S. at 217–27 (citing and quoting *Mayo* throughout).[8] Under the

[8] We are also guided by Office's *2019 Revised Patent Subject Matter Eligibility Guidance* ("Office Guidance"), which outlines the *Alice/Mayo* framework in terms of a three-part inquiry. 84 Fed. Reg. 50, 53–56 (Jan. 7,

Alice/Mayo framework, we consider, first, whether the claims recite an abstract idea, and, if so, whether the claims are otherwise directed to a technological improvement that transforms them into a "practical application" of the idea.[9] *Mayo*, 566 U.S. at 77–78, 84–85 (quoting *Gottschalk v. Benson*, 409 U.S. 63, 71 (1972)); *see also Alice*, 573 U.S. at 221–24 (evaluating whether computer implementation of a mathematical formula is "the sort of 'additional featur[e]' that provides any 'practical assurance that the process is more than a drafting effort designed to monopolize the [abstract idea] itself'") (alteration in original) (quoting *Mayo*, 566 U.S. at 77); *Diamond v. Diehr*, 450 U.S. 175, 187 (1981) ("It is now commonplace that an *application* of a law of nature or mathematical formula to a known structure or process may well be deserving of patent protection."). As a final safeguard, we consider whether any claim elements, either individually or in combination, amount to an "inventive concept," in other words, something "significantly more" than "well-understood, routine, conventional activities previously known to the industry."[10] *Alice*, 573 U.S. at 221–22, 225 (internal quotations, brackets, and citations omitted).

2019) (describing "Step 2A" as including "Prong One" and "Prong Two," followed by "Step 2B").

[9] This step of the *Alice/Mayo* framework is recounted in the Office Guidance as "Revised Step 2A . . . Prong One: Evaluate Whether the Claim Recites a Judicial Exception . . . [and] Prong Two: If the Claim Recites a Judicial Exception, Evaluate Whether the Judicial Exception is Integrated Into a Practical Application." 84 Fed. Reg. at 54.

[10] This step of the *Alice/Mayo* framework is recounted in the Office Guidance as "Step 2B: If the Claim is Directed to a Judicial Exception, Evaluate Whether the Claim Provides an Inventive Concept." 84 Fed. Reg. at 56.

1. Whether the Claims Recite an Abstract Idea

AvePoint asserts that the claims of the '090 patent are directed to "assessing the risk of personal data being compromised." Pet. 34; *see also id.* at 9 (characterizing the claims as directed to "determining the risk of personal data being compromised"). Even more specifically, according to AvePoint, the claims recite the steps of determining an overall risk level for a privacy campaign "by assessing . . . certain well-known risk factors and assigning values to the risk factors depending on the type of personal data entered as part of the campaign." Pet. 9; *see also* Pet. Reply 15–16 ("The key components of the '090 claims are the processor and the human mental processes, with the latter dictating the weight and risk values and the former tallying the inputs."). AvePoint analogizes "assessing the risk of personal data being compromised" to the abstract idea of "mitigating risk" held to be a patent-ineligible method of organizing human activity in *Alice* and *Bilski*. Pet. 31–32; *see also id.* at 10 (same). AvePoint also characterizes the claims as reciting a patent-ineligible "mental process."[11] *Id.* at 33; *see also* Pet. Reply 9–10 (conforming its assertions to "Groupings of Abstract Ideas" as defined in the Office Guidance).

Rather than respond to AvePoint's contention that the claims recite a mental process or a method of organizing human activity, OneTrust focuses on the question of whether the claims are directed to a "technical improvement" that integrates the abstract idea into a practical application.

[11] AvePoint further asserts that the claims are directed to yet a third category of abstract ideas—"mathematical concept." Pet. Reply 10 (citing Office Guidance). We need not reach that question for we decide that the claims more aptly recite an abstract idea in the form of either a mental process or a method of organizing human activity.

PO Resp. 69, 75, 79; Sur-Reply 20. But before considering that question, we must first determine if the claims recite an abstract idea such that we can then properly inquire whether the claims otherwise recite "additional features" that transform them into a "practical application" of the idea itself. *Mayo*, 566 U.S. at 77–78, 84–85 (quoting *Gottschalk*, 409 U.S. at 71); *see also Alice*, 573 U.S. at 221–24 (considering whether computer implementation of the abstract idea is "the sort of 'additional featur[e]' that provides any 'practical assurance that the process is more than a drafting effort designed to monopolize the [abstract idea] itself'") (quoting *Mayo*, 566 U.S. at 77).

At the outset, we note that OneTrust does not dispute that the claims recite the idea of risk assessment—"we do not dispute that this claim involves risk assessment. That is the industry and the purpose of this software. But what the software is claiming is an improved method of implementing a risk assessment that uses two different factors in order to enable the software to be customized." Tr. 50:15–19; *see also* PO Resp. 74 ("There is no dispute that privacy risk assessments had been performed on computers prior to the '090 patent."). More specifically, according to OneTrust, the claimed method "determine[s] a risk level for a privacy campaign (i.e., a project or process that may utilize personal data) based on two separate metrics—a 'weighting factor' and a separate 'relative risk rating' for each of a plurality of risk factors." PO Resp. 74–75. Indeed, claims 1 and 21 include steps that relate directly to conducting a privacy risk assessment—

> (1) "receiving campaign data input by one or more users,"
>
> (2) "determining a weighting factor for each of a plurality of risk factors" associated with the campaign data,

> (3) "determining a relative risk rating for each of the plurality of risk factors," and
>
> (4) "calculating a risk level for the campaign based upon . . . the relative risk rating for the respective risk factor and the weighting factor for the risk factor."

Ex. 1001, 34:34–35:32.

Those steps of assessing the risk of personal data being compromised by associating certain risk factors with the data and then rating and weighing each factor to generate an overall "risk level," as recited in claims 1 and 21, amount to nothing more than a mental process that can be performed in the human mind or by a person using pen and paper. For instance, the "receiving" step can be performed by a person who simply reads the personal data and records certain items of information from the data. The "determining" steps can be performed by a person who associates risk factors with the chosen data and writes a value "from 1–10" on paper in rating each risk factor (*see, e.g.*, Ex. 1001, 20:30–33) and writes a value "from 1–5" on paper in weighing each risk factor. *See id.* at 19:21–23, 20:19–22, 20:30–33. Lastly, the "calculating" step can be performed by a person who simply multiplies and adds the assigned values for each risk factor, be it on paper or in her head, to arrive at an overall risk level for the personal data. *See id.* at 4:64–5:7, 36:35–37. Notably, OneTrust's own expert confirmed that each of these steps can be performed mentally. Ex. 1030, 48:9–50:14[12] (confirming that a "person" may determine and enter the "relative risk rating" and "weighting factor," then "multiply" one by the other, "and then add them together").

[12] Citations for Exhibit 1030 are to original page numbers of the deposition transcript.

Moreover, this series of steps is plainly directed to the long-standing and fundamental business practice of assessing and mitigating the risk of personal data being compromised. Indeed, the '090 patent acknowledges as much in the "Background" section—

> *Many regulators recommend conducting privacy impact assessments, or data protection risk assessments along with data inventory mapping.* For example, the GDPR [European Union's General Data Protection Regulation] requires data protection impact assessments. Additionally, the United Kingdom ICO's office provides guidance around privacy impact assessments. The OPC in Canada recommends personal information inventory, and the Singapore PDPA specifically mentions personal data inventory mapping.
>
> Thus, developing operational policies and processes may reassure not only regulators, but also an organizations customers, vendors, and other business partners.
>
> *For many companies handling personal data, privacy audits,* whether done according to AICPA Generally Accepted Privacy Principles, or ISACA's IT Standards, Guidelines, and Tools and Techniques for Audit Assurance and Control Professionals, *are not just a best practice, they are a requirement.*

Ex. 1001, 2:9–26 (emphases added). That description in the '090 patent shows that, for many organizations, assessing the risk of personal data being compromised is not only a generally accepted business practice, but a legal requirement. Indeed, OneTrust's own expert testifies that risk assessments include "basic steps that have been around" since well before the 2016 priority date of the '090 patent. Ex. 1030, 25:24–30:19. She likewise confirms that "risk assessments" of "privacy campaign[s]" are common in the "business process" and "have been around for many, many years." *Id.* at 53:9–22. That the fundamental business practice of assessing the risk of personal data being compromised is an abstract idea comports fully with the

"fundamental economic practice" of "hedging, or protecting against risk" determined to be an abstract idea in *Bilski* (561 U.S. at 611–12), as well as the "mitigat[ing] settlement risk" determined to be an abstract idea in *Alice* (573 U.S. at 219–20).

The claims here are not unlike the claims held to be abstract in *FairWarning IP, LLC v. Iatric Systems, Inc.*, 839 F.3d 1089, 1095 (Fed. Cir. 2016). In that case, the claims were held to be abstract 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. *Id.* at 1093–94 (citing *Alice*, 573 U.S. at 220). Like the case here, the claimed method in *FairWarning* included the general steps of collecting information that included personal data, processing and analyzing the information according to certain rules and criteria 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, they nonetheless were held to be abstract 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 is also the case here. As such, we determine that the claims recite an abstract idea.[13]

[13] Our determination is consistent with the Office Guidance's identification of "mitigating risk" as a "method of organizing human activity" and "concepts performed in the human mind" as "[m]ental processes," each of which is an abstract idea. 84 Fed. Reg. at 52 n.13 (citing *Alice* and *Bilski*), n.14 (citing *CyberSource Corp. v. Retail Decisions, Inc.*, 654 F.3d 1366 (Fed. Cir. 2011)).

2. Whether the Claims Include Additional Elements that Integrate the Abstract Idea into a Practical Application

Having determined that the claims recite an abstract idea, we now consider whether the claims include "additional features" that transform the idea into a "practical application." *Mayo*, 566 U.S. at 77–78, 84–85 (quoting *Gottschalk*, 409 U.S. at 71). Additional features indicative of a practical application typically reflect "a specific improvement to the way computers operate" or "a specific implementation of a solution to a problem in the software arts," which go beyond invoking a computer "merely as a tool." *Enfish, LLC v. Microsoft Corp.*, 822 F.3d 1327, 1336, 1339 (Fed. Cir. 2016).

OneTrust relies heavily on this prong of the § 101 analysis to argue that the claims are not directed to a patent ineligible abstract idea. PO Resp. 74–87; Sur-Reply 17–22; Tr. 49:13–51:20, 64:19–65:16. According to OneTrust, rather than being directed to an abstract idea, the claims are directed to a "technical improvement" or "solution" because "an organization (or operational unit within an organization) can customize the weighting factor and the relative risk rating to reflect the organization's own particular needs." PO Resp. 75. "Unlike prior software for performing privacy impact assessments," OneTrust explains, "the claimed methods allow OneTrust's software tool to be adjusted for different users' particular privacy sensitivities, thereby avoiding the need for custom built or in-house solutions." *Id.* As such, OneTrust surmises that the claims of the '090 patent "focus on an improvement in computer capabilities—namely, an improvement in the capabilities of software for performing privacy impact assessments *to be customized* for particular customer risk sensitivities or for different privacy regimes." *Id.* at 76 (emphasis added); *see also id.* at 77 ("Again, the claims are specifically directed to a method that improves the

functionality of a computer by allowing the software *to be adjusted* for different user needs or preferences regarding the relative risks posed by different risk factors." (emphasis added)).

But OneTrust's argument relates to "user customizations" of information stored in the database—namely, the "weighting factors" and "risk rating"—for use by a "Risk Assessment Module" in calculating the overall risk level. Ex. 1001, 20:10–35. In that regard, the Specification explains that the "Risk Assessment Module," which determines the overall risk level, "may have default settings" or "[t]he organization may also modify these settings in the Risk Assessment Module." *Id.* at 19:25–32. Elaborating further, the Specification states that those settings "may be customized from organization to organization, and according to different applicable laws." *Id.* at 18:58–67. In other words, the user may modify the default settings of the risk rating and weighting factor according to the particular needs of the organization conducting the privacy campaign.

That the user organization may modify the default settings in the Risk Assessment Module reflects simply a benefit to the user's input of information, not an improvement to the database's functionality. As the Federal Circuit has held, while the ability of a user to select "classifications, parameters, and values" for information within a database "improves the quality of the information added to the database, an improvement to the information stored by a database is not equivalent to an improvement in the database's functionality." *BSG Tech LLC v. BuySeasons Inc.*, 899 F.3d 1281, 1288 (Fed. Cir. 2018). In the end, AvePoint's claimed invention merely "results in better user input, but the database serves in its 'ordinary capacity' of storing the resulting information." *Id.* (citing *Enfish*, 822 F.3d

at 1336). Thus, we agree with AvePoint that claims 1 and 21 are not directed to a technological improvement to database functionality, but rather any benefit flows from performing the abstract idea in conjunction with the entry of long-standing criteria for risk assessments.

Moreover, that a "weighting factor" and a "risk rating" are long-standing criteria in assessing the risk to data privacy is borne out by testimony from both parties' experts. For instance, AvePoint cites persuasive testimony from its expert that assigning "weight" and "rating" values to various risk factors was "part of the state of the art." *See, e.g.*, Ex. 1002 ¶¶ 49–51 (citing Exs. 1005–1008). Indeed, one of the prior art patents cited by AvePoint's expert expressly describes a "[c]onfiguration module" that allows an administrator to configure various parameters of reporting/scoring software," such as "weighting" factors and "degree of risk" ratings in scoring data privacy protections. Ex. 1005 ("McQuay"), 7:60–67, 8:66–9:13, 11:24–30. And, like the Risk Assessment Module in the '090 patent, McQuay's "configuration module" is "configured to allow an administrator *to modify the model used by reporting/scoring software . . . [and] define new models*."[14] *Id.* at 9:14–26 (emphasis added). Another prior art document cited by AvePoint's expert likewise discloses "evaluating and rating privacy risks" by applying a "Weight" and "Rating" to various risk factors ("privacy criteria . . . P1–P9") in the calculation of an overall risk level ("Overall Score"). Ex. 1006 ¶¶ 2, 41–56, 66, Table 1. Moreover,

[14] Also, like the '090 patent, McQuay speaks expressly of the need to "implement[] privacy protection measures to ensure proper handling of personal information" and "assess[] an organization's implementation of the privacy protection measures and its compliance with privacy protection legislation," such as Canada's "PIPEDA" law. Ex. 1005, 1:14–36.

OneTrust's own data privacy expert confirms that she routinely assigned weights of "[h]igh, medium, and low" to risk factors in conducting privacy risk assessments in the 2012–2015 timeframe. Ex. 1030, 33:16–34:24.

That contemporaneous evidence belies OneTrust's argument that the claimed "weighting factor" and "risk rating" somehow reflect "a functional improvement to software for operationalizing privacy compliance." Sur-Reply 17–18; *see also id.* at 21–22 (essentially same). If anything, the ability to modify the criteria stored in the database reflects an insignificant data gathering step that fails to elevate the claims beyond the abstract idea itself. *Ultramercial, Inc. v. Hulu, LLC*, 772 F.3d 709, 716 (Fed. Cir. 2014) (holding that "the steps of consulting and *updating* an activity log represent insignificant 'data-gathering steps,' . . . and thus add nothing of practical significance to the underlying abstract idea") (emphasis added)); *see also Accenture Global Servs., GmbH v. Guidewire Software, Inc.*, 728 F.3d 1336, 1345 (Fed. Cir. 2013) (holding that limitations reciting "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") (emphasis added)).

Finally, despite OneTrust's arguments to the contrary, the patent claims here are not analogous to the patent claims in *Finjan, Inc. v. Blue Coat Systems, Inc.*, 879 F.3d 1299 (Fed. Cir. 2018). PO Resp. 80–84; Sur-Reply 7, 18–20. Notably, the Specification of the '090 patent purports to have filled "a need for improved systems and methods for monitoring compliance with corporate privacy policies and applicable privacy laws." Ex. 1001, 2:40–42. But that goal is in the abstract realm—an improvement

in the fundamental business practice of assessing the risk of personal data being compromised—not an improvement in computer capabilities. In *Finjan*, the claims employed "a new kind of file that enables a computer security system to do things it could not do before." *Finjan*, 879 F.3d at 1305. As noted in *Finjan*, that new file was a "specific downloadable" that did not simply permit access "to be tailored for different users," as OneTrust repeatedly emphasizes (PO Resp. 80–83; Sur-Reply 18–19), but more importantly "ensures that threats are identified before a file reaches a user's computer," which OneTrust ignores entirely. *Finjan*, 879 F.3d at 1305.

Finjan cannot save the claims here, as they do not recite a new kind of file that allows the computer to do something it could not previously do. That the claims here list the use of long-standing criterion, such as "risk rating" and "weighting factor," in determining the risk level does not change the fact, that, as a whole, the claims are still directed to the abstract idea of assessing the risk of personal data being compromised. Indeed, the claims here merely require the manipulation of common data (personal data) by applying longstanding criteria (risk ratings and weighting factors) to arrive at a common determination (risk level). Although that criteria may change with the user of the software, it does not allow the computer to do something it could not previously do, namely, perform a risk assessment for a privacy campaign.

3. Whether the Claims Include an Inventive Concept

We next consider whether an element or combination of elements in the claims involve "significantly more" than the performance of "well understood, routine, conventional activities previously known to the industry." *Alice*, 573 U.S. at 222–23 (quoting *Mayo*, 566 U.S. at 78); *see*

also Berkheimer v. HP, Inc., 881 F.3d 1360, 1368 (Fed. Cir. 2018) ("The question of whether a claim element or combination of elements is well-understood, routine and conventional to a skilled artisan in the relevant field is a question of fact."). Here, AvePoint asserts that the independent claims recite nothing inventive 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 support its attorney argument with *actual evidence*" of the routine and conventional nature of the claims. PO Resp. 89. We disagree.

We find that AvePoint proffers sufficient proof that the claims recite only "generic" computer components to perform the well-known business practice of assessing the risk level of personal data being compromised. Pet. 36. Indeed, in our Institution Decision, we pointed to the Specification of the '090 patent as evidence that the "graphical user interface," "storage [location]," and "processors" are "conventional computer components." Inst. Dec. 11–12 (citing Ex. 1001, 2:64–3:4, 3:64–4:2 (describing "graphical user interface (GUI)"), 3:18–21, 10:9–11 (describing "computer-readable storage medium"), 11:53–67 (describing "general purpose processing devices")). OneTrust never disputes that evidence as to the well-understood, routine, and conventional nature of the components as claimed. *See* PO Resp. 87–91. Based on that undisputed evidence, we find that AvePoint has demonstrated that the generic computer components recited by claims 1 and 21 are not an inventive concept.

Nor is there any dispute that the claimed "risk factors" were well known in the relevant time frame. *See id.* In our Institution Decision, we

stated that the claimed "risk factors" are within the "norm of what would typically underlie a risk assessment of personal data being compromised." Inst. Dec. 11. In doing so, we agreed with AvePoint that the "Background" section of the '090 patent supports 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. *Id.* at 12 (citing Ex. 1001, 2:9–39). We also noted the unrebutted testimony of AvePoint's expert 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.* at 11–12 (citing Ex. 1002 ¶¶ 42–50). OneTrust has no response to the well-known nature of the claimed "risk factors." *See* PO Resp. 88–91; Sur-Reply 22–24. Given the description of the "risk factors" in the Background of the '090 patent, along with the unrebutted testimony of AvePoint's expert, we are persuaded that the "risk factors" as claimed do not amount to an inventive concept.

Rather than dispute the overwhelming evidence of the well-understood, routine, and conventional nature of the claimed generic components and "risk factors," OneTrust focuses on the claimed "risk rating" and "weighting factor" as providing the purported inventive concept. PO Resp. 88–89; Sur-Reply 22–24. In particular, OneTrust argues there is "no credible evidence" that "using both 'weighting factors' and 'relative risk ratings' for each of the 'plurality of risk factors' . . . were widely prevalent or in common use in the privacy management field" and cites to testimony from its expert in support of that proposition. PO Resp. 88 (citing Ex. 2008

¶¶ 58–59). But OneTrust's expert testifies that AvePoint's showing as to the state of the art "lacks facts, data, or evidentiary support." *See* Ex. 2008 ¶ 58 (citing Ex. 1002 ¶¶ 40–48).

More specifically, OneTrust's expert testifies that "¶¶ 40–48" of AvePoint's expert declaration lack "citations to evidence to support what was supposedly well known." *Id.* That testimony is inaccurate because AvePoint does not rely on paragraphs 40–48 of its expert declaration to show that the use of weighting factors and risk ratings were well known in the art. Instead, AvePoint relies expressly on paragraphs 49–51 of its expert declaration, which include the very citations to evidentiary support that OneTrust's expert inaccurately testifies are lacking. *See* Pet. Reply 16 (citing Ex. 1002 ¶¶ 49–51). Had OneTrust's expert not overlooked those paragraphs, she would have seen that AvePoint's expert actually cites supporting evidence for his testimony that assigning "weight" and "rating" values to various risk factors was "part of the state of the art." *See* Ex. 1002 ¶¶ 49–51 (citing Exs. 1005–1008).

In other words, contrary to OneTrust's reliance on inaccurate expert testimony, AvePoint provides ample evidentiary support in the form of credible expert testimony (Ex. 1002 ¶¶ 49–50) and contemporaneous patent documents (Exs. 1005–1011) to show that the use of weighting factors and risk ratings in assessing data privacy was well-known, routine, and conventional. Indeed, Exhibit 1005 describes expressly the "entry of percentage weights" and "degree of risk . . . according to a scale between 1 and 9" in scoring data privacy protections. Ex. 1005, 8:66–9:13, 11:24–30, Figs. 5A, 6. Because OneTrust's expert overlooks that evidence entirely, it remains unrebutted, and we find it persuasive. That cumulative evidence

belies OneTrust's argument that the claimed "weighting factor" and "risk rating" are an inventive concept. Instead, we find persuasive AvePoint's evidence that such criteria was well known, routine and conventional in data privacy assessments before the priority date of the '090 patent.

In sum, we determine that AvePoint demonstrates under *Alice* step two that all the limitations of the independent claims, individually and as ordered combinations, do not provide an inventive concept.

4. Whether Dependent Claims 2–20 and 22–25 Recite a Technological Improvement or Inventive Concept

The above analysis applies with equal force to the dependent claims. For these, AvePoint analyzes each of the dependent claims in arguing that they are also abstract and do not add anything of significance to the abstract idea of the claims 1 and 21. Pet. 38–40. According to AvePoint, the dependent claims lack an "end *result* to the functionality of a computer," and, instead, recite merely "insignificant extra-solution activity." Pet. Reply 14.

OneTrust responds that the dependent claims "have not been shown to be well-understood, routine, or conventional in the industry," and that AvePoint "has thus failed to meet its burden of showing that the dependent claims do not contain an inventive concept." PO Resp. 91–92; *see also* Sur-Reply 24 ("Petitioner failed to meet its burden."). For the following reasons, we disagree that AvePoint has not met its burden in showing that the claims are directed to an abstract idea and lack an inventive concept.

Dependent claims 2–6 relate to the users who input the campaign data of claim 1. Simply identifying the users who enter the campaign data does not elevate the claims into a technological improvement, but rather flows

directly from the performance of the abstract idea itself, which, as discussed above, is a mental process. Also, the routine "inputs" of campaign data recited by these claims amount to insignificant "data gathering" steps that fail to elevate the claims beyond the abstract idea itself. *Ultramercial*, 772 F.3d at 716. Thus, we are not persuaded that the limitations of dependent claims 2–6 transform the abstract idea into a patent-eligible application or an otherwise inventive concept.

Dependent claims 7–12 recite that the generic "graphical user interfaces" include "fields," "prompts" or "notifications" for the input of campaign data. As discussed above with respect to claims 1 and 21, the use of graphical user interfaces for the entry of campaign data was well understood, routine, and conventional before the priority date of the '090 patent. And we do not discern any meaningful language in claims 7–12 that might elevate such generic interfaces into something more than a routine and conventional feature for the entry of data. Rather, we find persuasive the testimony of AvePoint's expert that such interfaces were "state of the art" by the time of the '090 patent. *See* Ex. 1002 ¶¶ 38–39. As such, we find that the limitations of claims 7–12 do not transform the abstract idea into a patent-eligible application or an inventive concept.

Dependent claims 13 and 14 are directed to assigning a value to the weighting factor and using that value, along with the risk rating, to calculate the risk level. The only difference from claims 1 and 21 is that the calculation is described as the "sum" of all the weighting factors "multiplied" by the risk rating. As discussed above, AvePoint provides persuasive proof in the form of unrebutted expert testimony and contemporaneous patent documents that the calculation of risk level in this

manner "do[es] not improve computer functionality" but rather relates to "underlying principles of any fundamental risk assessment of operations using personal data." *See* Ex. 1002 ¶¶ 49–50, 52–53; Exs. 1005–1011. As with claims 1 and 21, that evidence persuades us that the limitations of claims 13 and 14 do not transform the abstract idea into a patent-eligible application or an inventive concept.

Dependent claims 15–19 relate to "retrieving" and "display[ing]" campaign data to a user. But "claims . . . devoted to . . . merely selecting information, by content or source, for collection, analysis, and display does nothing significant to differentiate a process from ordinary mental processes, whose implicit exclusion from § 101 undergirds the information-based category of abstract ideas," particularly where, as here, the dependent limitations "do not even require a new source or type of information, or new techniques for analyzing it." *Elec. Power Grp. LLC v. Alstom S.A.*, 830 F.3d 1350, 1355 (Fed. Cir. 2016); *see also Intellectual Ventures I LLC v. Capital One Bank (USA)*, 792 F.3d 1363, 1369 (Fed. Cir. 2015) ("Requiring the use of a 'software' 'brain' 'tasked with tailoring information and providing it to the user' provides no additional limitation beyond applying an abstract idea, restricted to the Internet, on a generic computer."). Thus, we determine that the limitations of claim 15–19 fail to transform the abstract idea into a patent-eligible application or an inventive concept.

Dependent claim 20 relates to the "type of individual" whose personal data is the subject of the privacy campaign. As such, it reflects an insignificant "data gathering" step that fails to elevate the claims beyond the abstract idea itself. *Ultramercial*, 772 F.3d at 716. Nor does this limitation add anything of significance to the idea itself. Thus, claim 20 fails to

transform the abstract idea into a patent-eligible application or an inventive concept.

Finally, claims 22–25 relate generally to "communications" for facilitating the input of campaign data, such as "an electronic message" in the form of "a question" or "remind[er]" that may be in "real-time." Again those limitations flow directly from performing the abstract idea itself, which, as discussed above, is a mental process. Quite simply, like many of the dependent claims, they add nothing of significance and are merely "data gathering" steps that fail to transform the abstract idea into a patent-eligible application or an otherwise inventive concept. *Id.*

In sum, while the dependent claims may narrow the scope of claims 1 and 21, they neither relate to the purportedly inventive concept of using a "weight factor" and "relative risk rating" in the calculation of a risk level, nor do they otherwise transform the abstract idea into a patent-eligible application of that concept.

5. Conclusion

After considering the entire record, we determine that AvePoint has demonstrated by a preponderance of the evidence that claims 1–25 do *not* recite patent eligible subject matter under 35 U.S.C. § 101, and thus, are unpatentable.

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

Because we determine that all the challenged claims are unpatentable under 35 U.S.C. § 101, we need not reach AvePoint's challenges on grounds of obviousness under 35 U.S.C. § 103(a).

D. AvePoint's Motion to Exclude

AvePoint seeks to exclude the declaration and deposition testimony of OneTrust's expert, namely. Mot. to Exclude 1. According to AvePoint, OneTrust's expert is "not qualified" and her testimony is "not based on sufficient facts or data." *Id.* We disagree.

OneTrust's expert testifies that she has been "a professional in the privacy software field since at least May 2012." Ex. 2008 ¶ 5. In that time, she has "focused on privacy assessments for digital banking," "help[ed] companies with . . . US privacy law compliance," and "spoken on data privacy to numerous conferences." *Id.* ¶¶ 8–10. Notably, she has "complete[d] over 100 privacy impact assessments," which, in our view, goes to the very heart of the claimed invention. *Id.* ¶ 11. As such, AvePoint does not persuade us that OneTrust's expert lacks qualification to testify in this proceeding. *See* Mot. to Exclude 4–13. Also, to the extent AvePoint contends that the testimony of OneTrust's expert lacks sufficient factual support, that contention goes to weight, not admissibility, of the testimony. *See id.* at 13–14. And we note the particular testimony of OneTrust's expert that we have accorded little weight. Moreover, to the extent we rely on her testimony in reaching this Final Written Decision, that testimony is not adverse to AvePoint. Thus, we deny AvePoint's motion to exclude.

E. OneTrust's Motion to Strike

OneTrust seeks to strike AvePoint's "belatedly presented declaration from a new expert" (Ex. 1032), as well as "new argument" from AvePoint as to "an implicit motivation to combine the prior art." Mot. to Strike 1. Because we neither rely on the objected-to declaration nor reach AvePoint's obviousness grounds, we deny OneTrust's motion to strike as moot.

III. CONCLUSION[15]

In summary:

35 U.S.C.	Claims	Claims Shown Unpatentable	Claims Not Shown Unpatentable
§ 101	1–25	1–25	
§ 103[16]	1–25		
Overall Outcome		1–25	

IV. ORDER

Accordingly, it is:

ORDERED that claims 1–25 of the '090 patent are held *unpatentable*;

FURTHER ORDERED that AvePoint's Motion to Exclude (Paper 34) and OneTrust's Motion to Strike (Paper 27) are *denied*; and

FURTHER ORDERED that, because this is a Final Written Decision, any party to the proceeding seeking judicial review of the decision must comply with the notice and service requirements of 37 C.F.R. § 90.2.

[15] Should OneTrust wish to pursue amendment of the challenged claims in a reissue or reexamination proceeding after issuance of this decision, we draw OneTrust's attention to the April 2019 *Notice Regarding Options for Amendments by Patent Owner Through Reissue or Reexamination During a Pending AIA Trial Proceeding. See* 84 Fed. Reg. 16,654 (Apr. 22, 2019). We further remind OneTrust of its continuing obligation to notify the Board of any such related matters in updated mandatory notices. *See* 37 C.F.R. § 42.8(a)(3), (b)(2).

[16] As discussed above, we do not reach this ground.

FOR PETITIONER:

Nathan A. Evans
Joshua F. P. Long
WOODS ROGERS PLC
nevans@woodsrogers.com
jlong@woodsrogers.com

FOR PATENT OWNER:

David A. Reed
Michael S. Pavento
KILPATRICK TOWNSEND & STOCKTON LLP
dreed@kilpatricktownsend.com
mpavento@kilpatricktownsend.com

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

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