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;

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS

Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS

Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS

Sync your system to PACER to automate legal marketing.

WHAT WILL YOU BUILD? | **sales@docketalarm.com** | **1-866-77-FASTCASE**