UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|---|---|---|---|---|
| 13/565,002 | 08/02/2012 | Yasutaka Nishimura | JP920100059US2 | 9517 |

37945 7590 07/03/2018
DUKE W. YEE
YEE AND ASSOCIATES, P.C.
P.O. BOX 802333
DALLAS, TX 75380

| EXAMINER | |
|---|---|
| WINTER, JOHN M | |

| ART UNIT | PAPER NUMBER |
|---|---|
| 3685 | |

| NOTIFICATION DATE | DELIVERY MODE |
|---|---|
| 07/03/2018 | ELECTRONIC |

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

ptonotifs@yeeiplaw.com
mgamez@yeeiplaw.com

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

*Ex parte* YASUTAKA NISHIMURA, TAKASHI OGURA,
AKIRA OHKADO, and TADASHI TSUMURA

Appeal 2017-002044
Application 13/565,002[1]
Technology Center 3600

Before CARLA M. KRIVAK, AMBER L. HAGY, and
PHILLIP A. BENNETT, *Administrative Patent Judges*.

BENNETT, *Administrative Patent Judge*.

## DECISION ON APPEAL

## STATEMENT OF THE CASE

Appellants appeal under 35 U.S.C. § 134 from the Examiner's final rejection of claims 1–21. We have jurisdiction under 35 U.S.C. § 6(b).

We affirm.[2]

[1] Appellants' Brief ("App. Br.") identifies International Business Machines Corporation as the real party in interest. App. Br. 1.

[2] Although we do not sustain all claim rejections, we sustain at least one ground of rejection for each pending claim. 37 C.F.R. § 41.50(a)(1).

CLAIMED SUBJECT MATTER

The claims are directed to managing access to assets associated with time-specific work orders based on a security policy that monitors the location of the asset. Spec. ¶¶ 9–10. Claim 1, reproduced below, is illustrative of the claimed subject matter:

> 1. A method of processing by a computer to manage an access right to at least one asset associated with at least one digital work order, the method comprising steps executed by the computer of:
>
> at a scheduled start time for a work order to be executed, or in response to reception of a report indicating a start of work for the work order to be executed or a report indicating a completion of work for a preceding work order to the work order to be executed:
>
> loading into a memory of the computer a security policy associated with the work order to be executed, or an asset associated with the work order to be executed, and
>
> starting to monitor a location of the asset associated with the work order to be executed; and
>
> generating an event for managing the asset in response to a fact that the loaded security policy is violated by the location, or a change in the location of the asset associated with the work order that was obtained by the monitoring.

App. Br. 32 (Claims Appendix).

REJECTIONS

Claims 1–21 stand rejected under 35 U.S.C. § 101 as being directed to ineligible subject matter.

Claims 1–21 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Ratcliff et al. (US 2008/0163347, published July 3, 2008)

("Ratcliff") and Mitchell et al. (US 8,321,253 B2, issued Nov. 27, 2012[3]) ("Mitchell").

## ANALYSIS

### Section 101 Rejection

### *Legal Standard for Patent-Eligibility*

In issues involving subject matter eligibility, our inquiry focuses on whether the claims satisfy the two-step test set forth by the Supreme Court in *Alice Corp. v. CLS Bank Int'l.*, 134 S. Ct. 2347 (2014). The Supreme Court instructs us to "first determine whether the claims at issue are directed to a patent-ineligible concept," *Alice*, 134 S. Ct. at 2355, and, in this case, the inquiry centers on whether the claims are directed to an abstract idea. If the initial threshold is met, we then move to the second step, in which we "consider the elements of each 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." *Id.* (*quoting Mayo Collaborative Servs. v. Prometheus Labs., Inc.*, 566 U.S. 66, 79, 78 (2012)). The Supreme Court describes the second step as a search for "an 'inventive concept'—*i.e.*, an element or combination of elements that is 'sufficient to ensure that the patent in practice amounts to significantly more than a patent upon the [ineligible concept] itself.'" *Id.* (quoting *Mayo*, 566 U.S. at 72–73).

[3] Although issued after the effective filing date of Appellants' application, Mitchell qualifies as prior art under 35 U.S.C. § 102(e) based on its filing date of June 24, 2009.

*The Examiner's Findings*

The Examiner rejects claims 1–21 under the two-step *Alice* framework. Under the first step, the Examiner finds the claims are directed to the abstract idea of "loading a security policy associated with a work order." Final Act. 2, 4. The Examiner finds the concept to which the claims are directed amounts only to "comparing new and stored info[rmation] and using rules to identify options, which corresponds to concepts identified as abstract ideas by the courts." Ans. 2. Analyzing the claims under the second step of the *Alice* framework, the Examiner finds the "additional claim limitations beyond the concepts of loading a security policy with a work order and monitoring the security policy are recited at a high level of generality and are recited as performing generic computer functions routinely used in computer applications." *Id*. at. 3. The Examiner further determines that considering the claim limitations as an ordered combination "adds nothing that is not already present when looking at the elements taken individually." *Id*. at. The Examiner explains that "[t]here is no indication that the combination of elements improves the functioning of a computer or improves any other technology." *Id*. at 3–4.

*Appellants' Arguments—Claim 1*

Appellants present several arguments in favor of eligibility. First, Appellants argue the Examiner has failed to follow the Office guidelines on eligibility because "loading a security policy associated with a work order" and similar concepts have "not been held by a precedent court as being an 'abstract idea'." App. Br. 6. Appellants characterize their invention as "directed towards a technique that uses an asset-location monitoring technique to dynamically generate an asset-managing event in response to the asset-location violating a security policy associated with the work-order or asset." App. Br. 7. Appellants contend the claimed concept is "inextricably tied to computer technology and distinct from the types of concepts found by the courts to be abstract" under *Alice* step 1. *Id.*

With respect to the Examiner's *Alice* step 2 determination, Appellants argue that "[c]laim 1 recites an inventive concept of managing an access right to an asset associated with a work order such that an event is generated in response to the fact that a security policy associated with such work order or asset is violated." App. Br. 8. Appellants argue there is a "*synergistic interplay*" that goes beyond "mere generic computer-implemented steps implemented by a generic computer" as evidenced by Appellants' analysis of the rejections made under 35 U.S.C. § 103. *Id.* at 8. Appellants also argue the Examiner's analysis of the claims as an "ordered combination" is flawed because "when viewing the combination of steps *interoperating together* . . . there is a synergistic interplay (1) between the work order and security policy, and (2) between the security policy violation (that is asset-*location* based) and the generation of an event for managing the asset whose 'location' caused the security policy violation to occur." Reply Br. 3–4. Appellants also dispute the Examiner's finding that the claimed invention does not improve the functioning of a computer, arguing that security management technology is improved by solving the problem of "asset-*location*-based security policy violations pertaining to a specific work order." *Id.* at 4.

### *Analysis—Claim 1*

We are not persuaded by Appellants' arguments, and we address each in turn. We disagree with Appellants that "loading a security policy associated with a work order" and similar concepts have "not been held by a precedent court as being an 'abstract idea'." App. Br. 6. We see substantial similarity between this concept and the concept found abstract in *FairWarning IP, LLC v. Iatric Sys.*, 839 F.3d 1089 (Fed. Cir. 2016) ("*FairWarning*"). There, the Federal Circuit considered the eligibility of claims directed to fraud detection and misuse of computer information. The claim at issue in *FairWarning* recited:

> A method of detecting improper access of a patient's protected health information (PHI) in a computer environment, the method comprising:
>
> generating a rule for monitoring audit log data representing at least one of transactions or activities that are executed in the computer environment, which are associated with the patient's PHI, the rule comprising at least one criterion related to accesses in excess of a specific volume, accesses during a pre-determined time interval, accesses by a specific user, that is indicative of improper access of the patient's PHI by an authorized user wherein the improper access is an indication of potential snooping or identity theft of the patient's PHI, the authorized user having a pre-defined role comprising authorized computer access to the patient's PHI;
>
> applying the rule to the audit log data to determine if an event has occurred, the event occurring if the at least one criterion has been met;
>
> storing, in a memory, a hit if the event has occurred; and
>
> providing notification if the event has occurred.

*FairWarning IP*, 839 F.3d at 1092. Thus, like the claim at issue here, the claim found ineligible by the Federal Circuit in *FairWarning* was directed to a computer-based method that implements security policies ("authorized user having a pre-defined rule comprising authorized computer access") based on scheduled times ("accesses during a predetermined time interval") that detects violations of those policies ("indicative of improper access") with respect to an asset ("patient's PHI") and generates a notification when such unauthorized access occurs ("providing notification if the event has occurred"). As such, we agree with the Examiner that Appellants' claim 1 is similar to those previously found abstract by the courts, and we are not persuaded by this argument.

We also are not persuaded by Appellants' argument that claim 1 is not abstract because tracking an asset's location results in an invention "inextricably tied to computer technology and distinct from the types of concepts found by the courts to be abstract." App. Br. 7. In finding the *FairWarning* claims abstract, the Federal Circuit noted the "claims merely implement an old practice in a new environment." *FairWarning IP*, 839 F.3d at 1094. Here, the claimed location-tracking concept is little different from the longstanding practice of using retail security systems with clothing alarm tags to ensure items of clothing are not removed and stolen from a store. As such, the claim here, as was the case in *FairWarning*, merely implements an old practice in a new environment.

We also are unpersuaded by Appellants' contentions with respect to *Alice* step 2. As we noted above, Appellants argue claim 1 reflects an inventive "synergistic interplay" that goes beyond "mere generic computer-implemented steps implemented by a generic computer." Reply Br. 3–4. Appellants' contention is undermined by various statements made in the Specification. In describing the allegedly inventive location-based asset security policy, the Specification indicates determining the location of an asset was well-known and conventional. For example, the Specification states "[a]n appropriate technique known to a person skilled in the art may be used for obtaining the location, location change, or the elapsed time at a certain position." Spec. ¶ 34. The Specification also teaches that "a location detection engine known to a person skilled in the art may be used for the location detection means." Spec. ¶ 151.

Thus, the key technological innovation relied upon by Appellants—determining security violations based on location—is implemented using techniques and means "known to a person skilled in the art." We also note our reviewing court recently stated that to pass muster under *Alice* step 2, "[w]hat is needed is an inventive concept in the non-abstract realm." *SAP Am., Inc. v. InvestPic, LLC*, No. 2017-2081, 2018 U.S. App. LEXIS 12590, Slip. Op. 13 (Fed. Cir. May 15, 2018). Here, the alleged inventive concept closely tracks the abstract idea. Indeed, Appellants' characterization of the claims as embodying an "inventive concept of managing an access right to an asset associated with a work order such that an event is generated in response to the fact that a security policy associated with such work order is violated" is simply another way of saying the invention is directed to implementing security policies for work orders, which, as we noted above, is abstract. Accordingly, we agree with the Examiner that, considering the limitations as an ordered combination, the claim does not amount to significantly more than the abstract idea itself, and we therefore sustain the rejection of claim 1 under 35 U.S.C. § 101.

*Dependent Claims 2–10*

Appellants present separate arguments for patent-eligibility of claims 2–8 and 10, which depend from claim 1. For each claim, Appellants submit two arguments. First, they "urge error in the rejection of [the claim] for reasons given above with respect to Claim 1 (of which [the claim] depends upon)." *See, e.g.,* App. Br. 9 (claims 2, 3), 10 (claims 4, 7), 11 (claims 8, 10).[4] Second, Appellants characterize the functionality of each claim and argue the functionality "is not a generic computer-implemented step, as further described below in the 35 U.S.C. § 103 analysis." *See id.* Because Appellants have not shown error in the Examiner's conclusion with respect to claim 1, we are not persuaded by the first argument.

We also are not persuaded by Appellants' contentions regarding the functionality in each of claims 2–10 not being a "generic computer-implemented step, as further described below in the 35 U.S.C. § 103 analysis." It is well-established that patent-eligibility under *Alice* step 2 and patentability under section 35 U.S.C. §§ 102 and 103 are separate and distinct inquiries. *Two-Way Media Ltd v. Comcast Cable Communs., LLC*, 874 F.3d 1329, 1340 (Fed. Cir. 2017) ("Eligibility and novelty are separate inquiries."). Merely arguing that claims involve an inventive concept because they are allowable over prior art is insufficient to establish eligibility. Accordingly, we are not persuaded the Examiner erred in determining dependent claims 2–10 are ineligible under 35 U.S.C. § 101.

### *Independent Claim 11*

Appellants primarily argue that independent claim 11 is eligible "for similar reasons to those given above with respect to Claim 1." App. Br. 11. We do not find this argument persuasive for the reasons discussed above. Appellants further argue the Examiner erred because "[t]he Examiner fails to address the moving-object aspects of Claims 11 – which advantageously improves upon the art of security managements . . . ." App. Br. 11. We are not persuaded of Examiner error. Although slightly different in scope, we agree with the Examiner that claim 11 is, just as claim 1, directed to the

[4] Claim 9 is not argued separately, and it falls with claim 1.

abstract idea of "loading a security policy associated with a work order." Like claim 1, claim 11 is directed to a concept bearing substantial similarity to that found abstract in *FairWarning*. Moreover, as was the case with claim 1, the features relied upon by Appellants to argue the claim is not abstract—tracking the location of moving objects the duration of the object in a location—are implemented using techniques and means "known to a person skilled in the art." Spec. ¶ 34 ("An appropriate technique known to a person skilled in the art may be used for obtaining the location, location change, or the elapsed time at a certain position."). Accordingly, we are not persuaded independent claim 11 possesses sufficient inventiveness such that the *Alice* inquiry leads to a different result.

### *Dependent Claims 12–19 and 21*

Appellants present separate arguments for patent-eligibility of claims 12–19 and 21, which depend from claim 11.[5] App. Br. 12–13. The arguments for these claims largely reiterate the arguments presented for dependent claims 2–8 and 10, discussed above. For the same reasons, we are not persuaded by these arguments.

## SECTION 103 REJECTIONS

### *Independent Claim 1*

In rejecting claim 1, the Examiner finds the limitations are taught by the combination of Ratcliff and Mitchell. The Examiner relies on Ratcliff for teaching using access rights and loading security policies in connection with controlled access points. Final Act. 5–6; Ans. 9. The Examiner relies on Mitchell for teaching using work orders and scheduling work orders for

[5] Claim 20 is not argued separately, and it falls along with claim 11.

assets. Final Act. 6; Ans. 8–9. The Examiner finds a person of ordinary skill in the art would have combined Ratcliff and Mitchell "in order to schedule a work order for a client." Final Act. 6.

Contesting the rejection of claim 1, Appellants present four arguments. First, Appellants argue the references do not teach or suggest the recitation in the preamble of "at least one asset associated with at least one digital work order." Specifically, Appellants argue the work orders taught by Ratcliff are not "executed" as required by the language in the preamble, do not have any "asset" associated with them, and are not associated with a "security policy." App. Br. 15.

Second, Appellants argue the prior art fails to teach or suggest "generating an event for managing the asset *in response to* *a fact that the loaded security policy is violated* . . . ." App. Br. 16 (citing Ratcliff ¶ 23). Appellants contend Ratcliff fails to teach generating any managing event that is invoked or triggered based on a location-induced security policy violation. According to Appellants, Ratcliff merely describes control access points and information included in access rights files. *Id.* at. 16 (citing Ratcliff ¶ 26).

Third, Appellants contend the references do not teach "loading into a memory of the computer a security policy associated with the work order to be executed, or an asset associated with the work order to be executed." *Id.* at 17. Appellants argue the portions of Mitchell cited by the Examiner in the final Office Action make no reference to any security policy, and merely describe scheduling and monitoring the progress of work orders. *Id.* at. 18–19.

Finally, Appellants challenge the rationale for combining Ratcliff and Mitchell. Appellants argue the Examiner has failed to articulate any reasoning because the rationale provided is conclusory. *Id.* at. 19–20.

We are not persuaded by Appellants' arguments, and we address each argument in turn. However, before we turn to the merits of Appellants arguments, we first address a point of contention raised by Appellants in the Reply Brief. In the Reply Brief, Appellants argue the Examiner made new determinations and analysis in the Answer. *See, e.g.,* Reply Br. 9. Appellants argue that the reliance by the Examiner on these allegedly new grounds proves the rejection in the Final Action was deficient. Appellants, accordingly, argue that the Answer includes several new grounds of rejection; Appellants do not, however, request remand to the Examiner to reopen prosecution, but instead ask for reversal based on the state of the rejection in the Final Action while also presenting arguments purporting to show error in these allegedly new grounds.

Appellants' assertion that the Board should reject the Examiner's allegedly new arguments as untimely (Reply Br. 6) is contrary to the guidance provided by MPEP § 1207.03(b), based on 37 C.F.R. § 41.40, which sets out the exclusive procedure for an appellant to request review of the primary examiner's failure to designate a rejection in the Answer as a new ground of rejection via a petition to the Director under 37 C.F.R. § 1.181:

> [37 C.F.R. § 41.40] sets forth the exclusive procedure for an appellant to request review of the primary examiner's failure to designate a rejection as a new ground of rejection via a petition to the Director under [37 C.F.R. § 1.181], This procedure should be used if an appellant feels an answer includes a new ground of rejection that has not been designated as such and wishes to

> reopen prosecution so that new amendments or evidence may be submitted in response to the rejection. However, if appellant wishes to submit only arguments, the filing of a petition under [37 C.F.R. § 1.181] would not be necessary because appellant may submit the arguments in a reply brief. Any such petition under [37 C.F.R. § 1.181] must be filed within two months from the entry of the examiner's answer and prior to the filing of a reply brief.

MPEP § 1207.03(b). As Appellants did not petition to reopen prosecution, the Examiner's rejection, including the determinations and analysis from the Answer, are before us in the record.

Turning back to the merits of Appellants' arguments, we are not persuaded by Appellants' argument that the prior art references fail to teach or suggest "at least one *asset* associated with at least one digital work order." App. Br. 15. The Examiner finds, under the broadest reasonable interpretation of the term "asset," the technicians assigned work orders in Ratcliff teach an "asset associated with at least one digital work order." Ans. 9 (citing Ratcliff ¶¶ 23, 25, 26). We agree with the Examiner that the broadest reasonable interpretation of "asset" encompasses Ratcliff's technicians. The Specification does not provide a definition for "asset," nor does it exclude humans from being "assets." Moreover, the Examiner's broad interpretation is consistent with the dictionary definition for the term which provides that "asset" means "a useful or valuable thing, person, or quality." *Asset*, New Oxford American Dictionary 3d Ed., p. 96 (2010). Thus, we are not persuaded the Examiner erred in finding Ratcliff teaches the recited "asset associated with at least one digital work order." We also agree with the Examiner that the recited work order is "to be executed" as taught by Ratcliff's disclosure that a technician shows up for an "assigned shift" by arriving at "the section of Building A in which their assigned production line operates" (Ratcliff ¶ 26). Finally, we also agree that Ratcliff's "work order" has "a security policy" because it teaches access to the location of the production line may be limited to specific workers and specific times. Ratcliff ¶ 25. Accordingly, we are not persuaded by Appellants' first argument.

Appellants' second argument that Ratcliff does not teach the "generating" limitation of claim 1 is also unpersuasive. Appellants argue Ratcliff does not describe any event that is generated in response to a violation of a security policy due to the location of the asset. App. Br. 16; Reply Br. 9–10. We agree with the Examiner, however, that Ratcliff's teachings are sufficient to render obvious this limitation. Ratcliff teaches a security policy that is based on the location of an employee because if the employee is not at the correct building (i.e., location), an access right is not granted to the employee. Ratcliff ¶ 26. A person of ordinary skill in the art would have appreciated that enforcement of the location policy would have entailed generating an event such as setting a keycard to prevent them from entering a location in violation of the policy.[6] Accordingly, we agree with the Examiner that the teachings of Ratcliff are sufficient to render obvious the "generating" limitation of claim 1.

Appellants' third argument also fails to persuade us of error. Appellants argue Mitchell does not disclose the use of any security policy. App. Br. 17–19. However, the Examiner also relies on Ratcliff for the recited security policy (Ans. 9), a finding with which we agree. As we noted

[6] We note that Ratcliff teaches "[c]ontrolled access points may require the use of keys, codes, biometric, or other devices by which the controlled access point may restrict or control access." Ratcliff ¶ 23.

above in connection with Appellants' second argument, Ratcliff teaches the use of a security policy that is associated with both a work order (i.e., the requirement that an employee work at a particular location) and an asset (i.e., the employee). As such, we agree with the Examiner that Ratcliff teaches the "loading a security policy" limitation, and we are not persuaded by Appellants argument.

We find Appellants' fourth argument—that the Examiner has not provided an adequate rationale for combining Ratcliff and Mitchell—to be unpersuasive. Appellants merely assert that the Examiner's proffered rationale is "conclusory" and violates the requirement of "some articulated reasoning with some rational underpinning." App. Br. 19–20. However, Appellants do not explain how or why the Examiner's rationale is deficient. The Examiner finds a person of ordinary skill in the art would have sought to supplement Ratcliff's system with Mitchell to add a scheduling component as taught by Mitchell. Final Act. 6. We discern no error in this determination. As we explained above, Ratcliff teaches managing access rights in connection with work assignments, workers, and work facilities. *See, e.g.,* Ratcliff ¶ 23–27. Mitchell teaches the use of scheduling operations in connection with work orders. Mitchell, Abstract. Mitchell also teaches "[s]cheduling and dispatch services may help to manage a mobile technician workforce." Mitchell col. 1, ll. 16–18. An ordinarily skilled artisan would have appreciated the benefit of adding a scheduling component to Ratcliff because it is beneficial to provide scheduling in managing a workforce. Without an explanation of why a skilled artisan would have been dissuaded from doing so, we are not persuaded the Examiner erred in combining the pertinent teachings of Ratcliff and Mitchell.

Because we are not persuaded by Appellants' arguments with respect to independent claim 1, we sustain its rejection under 35 U.S.C. § 103.

*Claim 2*

Claim 2 depends from claim 1 and recites the limitation "in response to the generation of the event, cancelling or invalidating an access right to at least one access control device associated with an access to the asset associated with the work order already started." App. Br. 32 (Claims Appendix). The Examiner finds claim 2 is unpatentable as obvious in light of Ratcliff's description of terminating employee access when an employee leaves. Ans. 11 (citing Ratcliff ¶ 68). Appellants contend the Examiner has erred in two respects. First, Appellants argue an employee leaving is not equivalent to the claimed "event" because the recited event is "generated" and an employee leaving is not "generated/performed *in response to* a security policy violation." Reply Br. 12. Appellants also argue the termination of the employee's access right disclosed by Ratcliff is not the same as the claim because it "fails to address *what* the specific 'access right' of Claim 2 pertains to – that being an access right to at least *one 'access control device' associated with an access to the asset associated with the work order*." Reply Br. 12.

We are not persuaded by Appellants' argument. The cited portion of Ratcliff teaches that access rights can be granted and revoked with respect to specific areas or locations of a building. Ratcliff ¶ 68. Moreover, as we noted above in connection with claim 1, a person of ordinary skill in the art would have understood the "event" generated in response to a security policy violation such as disabling a keycard or other access control device to prevent the employee from entering a location in violation of the policy.

Taken together, these teachings at least suggest that when an employee (asset) attempts to enter a restricted area, their access to an access control device (keycard and lock) can be restricted or revoked. Accordingly, we are not persuaded the Examiner erred in rejecting claim 2, and we sustain its rejection.

### *Claim 3*

Claim 3 depends from claim 1 and recites the limitation "in response to the generating of the event, monitoring the asset violating the security policy by a monitor zooming-in, panning, or viewpoint adjustment on the asset associated with the at least one digital work order." App. Br. 32–33 (Claims Appendix). In rejecting claim 3, the Examiner does not find this limitation taught in any reference, but instead takes Official Notice that the limitation is "common and well known in prior art in reference to security to utilize video surveillance in order to detect intrusion of personnel into unauthorized areas." Final Act. 7. In response to Appellants' challenge to the Examiner cites U.S. Patent No. 6,727,938 ("Randall").

Appellants argue the Examiner improperly failed to substantiate the assertion of Official Notice despite Appellants' demand to do so in a response filed September 17, 2015, and that the teachings of Randall are inapposite. We agree. As noted by Appellants, Randall's abstract merely describes the use of rotatable surveillance cameras, and the language of claim 3 requires more than mere video surveillance. Reply Br. 13. Rather claim 3 requires monitoring during a specific situation—when an asset violates a security policy. Randall is not sufficient to substantiate the

Examiner's assertion of Office Notice of claim 3, and we do not sustain the rejection under 35 U.S.C. § 103.[7]

*Claim 4*

Claim 4 depends from claim 1 and recites the limitation "stopping or interrupting the monitoring at a scheduled completion time for the work order, or in response to reception of a report indicating the completion of work for the work order or a report indicating the start of work for a succeeding work order to the work order already started." App. Br. 33 (Claims Appendix). Here, again, the Examiner relies on Official Notice (Final Act. 7), and again Appellants challenge the Examiner's assertion (App. Br. 22). Unlike, claim 3, where the Examiner responded to Appellants' challenge, with respect to claim 4, the Examiner merely states "the rejection of Claim 4 is proper for reasons given above with respect to Claim 1 (of which Claim 4 depends upon)." Ans. 12. The Examiner's conclusion with respect to claim 4 is erroneous for two reasons. First, the Examiner has failed to respond to Appellants' demand for substantiation of the assertion of Official Notice. Second, because claim 4 is a dependent claim, it is by definition, narrower than claim 1 and includes additional limitations that must be taught or suggested by the prior art in order to be found unpatentable. As such, the Examiner's reasons for rejecting claim 1 are not, standing alone without any citation to prior art (due to the reliance on Official Notice), sufficient to reject claim 4. Accordingly, we do not sustain the rejection of claim 4 under 35 U.S.C. § 103.

[7] Although Randall is insufficient to substantiate an assertion of Official Notice, we express no opinion on whether it would, as part of a proper combination under § 103, be sufficient to render obvious the limitation of claim 3.

### *Claim 5*

Claim 5 depends from claim 1 and recites the limitation "wherein the event changes depending on a level or a type of security policy violation." The Examiner finds this limitation taught by Ratcliff. Final Act. 7 (citing Ratcliff ¶¶ 23, 26). In the Answer, the Examiner further finds this limitation disclosed in paragraph 61 of Ratcliff.[8] Ans. 12. Appellants argue claim 5 requires that the "event" generated in response to a security policy violation in claim 1 changes based on the type or level of the violation. App. Br. 22. Appellants further contend the Examiner has not identified any specific teaching in the cited paragraphs that demonstrates any change in the event based on the nature of the violation. *Id.* Appellants further contend the newly cited passage in the Answer is also insufficient because it merely describes that "people (primary data owners) change access rights for other people (John Doe/Jane Smith)." Reply Br. 13–14. We agree with Appellants. Although Ratcliff discusses revoking access rights for employees, the cited passage does not provide any indication that the nature of that revocation depends on a type or level of security policy violation. As such, we are persuaded the Examiner has erred in concluding claim 5 is obvious, and we do not sustain the rejection under 35 U.S.C. § 103.

### *Claim 6*

Claim 6 depends from claim 1 and recites the additional limitation "wherein the event changes depending on the work order or the asset." App. Br. 33 (Claims Appendix). The Examiner rejects claim 6, again citing the

[8] As we noted above, because Appellants did not petition the director to designate the Examiner's additional finding as a new ground, the aspect of the rejection is properly before us.

teachings of Ratcliff. Final Act. 7–8 (citing Ratcliff ¶¶ 23, 26). Appellants argue the Examiner has erred because the cited passages merely disclose control access points and access rights files. We are not persuaded by Appellants' argument. As we explained in connection with claim 1, the "asset" in Ratcliff is the employee, the "work order" is the employee's obligation to work at a particular location and time. The generated "event" enforcing the location policy would have entailed generating an event such as disabling a keycard to prevent the specific employee from entering a location in violation of the policy. Because the event would have been specific to the employee, Ratcliff teaches or suggests that the event "changes depending on the . . . asset." Accordingly, we are not persuaded the Examiner erred in rejecting claim 6, and we sustain the rejection under 35 U.S.C. § 103.

### *Claim 7*

Claim 7 depends from claim 1 and recites the limitation "wherein the event notifies a work manager of the security policy violation and includes evidence of the security policy violation with recorded content before the security violation occurred having been removed." App. Br. 33 (Claims Appendix). The Examiner finds this limitation taught by Ratcliff. Final Act. 8 (citing ¶¶ 39–40). In the Answer, the Examiner also determines the limitation recited in claim 7 is not entitled to patentable weight because it "merely states the result of the limitations in the claim [and] adds nothing to the patentability or substance of the claim." Ans. 13 (case citations omitted).

Appellants contend the cited paragraphs of Ratcliff do not teach the limitation of claim 7. App. Br. 24–25. Specifically, Appellants argue paragraph 39 of Ratcliff describes "generating a 'record' when a segregation of duties conflict has been identified." App. Br. 25. Appellants argue the record discussed in paragraph 39 is unrelated to the events described in paragraphs 23–26 relied upon by the Examiner. Appellants further argue that although paragraph 40 of Ratcliff describes the use of notifications, those notifications are dissimilar to the claim because they do not provide any notification of a security policy violation. App. Br. 25. Appellants further argue the Examiner's failure to accord the limitation patentable weigh is in error because the cases relied upon by the Examiner do not support such an interpretation. Reply Br. 14–16.

As an initial matter, we are persuaded the Examiner erred in finding the claim is not entitled to patentable weight. Appellants' have persuasively distinguished this situation from the cases cited by the Examiner. *See* Reply Br. 15–16. However, we are not persuaded that the teachings of Ratcliff do not render claim 7 obvious. We first note that the "recorded content" need not be video content, and as such, the recited "evidence of the security policy violation" may include various forms of "recorded content." We further note the cited passages in Ratcliff indicate that it was known to record information and provide notifications to data owners (i.e., supervisors) regarding anomalous security situations. Although the example described in Ratcliff paragraph relates specifically to "a segregation of duties conflict," a person of ordinary skill in the art would have appreciated that this content recording and notification procedure could be utilized in connection with the security violations taught in Ratcliff ¶¶ 23–26. As such, we are not persuaded the Examiner erred in rejecting claim 7, and we sustain the rejection under 35 U.S.C. § 103.

*Claim 8*

Claim 8 depends from claim 1 and recites the limitation "further comprising applying, responsive to a change in the security policy associated with the work order, a worker entity security policy associated with the worker entity designated in the work order to be executed." App. Br. 33 (Claims Appendix). In rejecting claim 8, the Examiner relies on paragraphs 26 and 47 of Ratcliff. Final Act. 8; Ans. 13.

Appellants argue Ratcliff fails to teach or suggest any "worker entity security policy" because the description in paragraph 26 only describes access rights and access rights files. App. Br. 26. Appellants further argue that the cited passage in paragraph 47 is deficient because it only teaches changing access rights for employees when needed. Reply Br. 17. We agree. Although the Examiner cites two passages of Ratcliff in support of the rejection, the Examiner provides no explanation for how those paragraphs teach the specific limitations. The Examiner merely states that the rejection of claim 8 "is proper for reasons given above with respect to Claim 1 which is in parallel with claim 8." Ans. 13. This reasoning is insufficient, and together with the Examiner's failure to explain the mapping of the cited paragraphs to the specific limitations in the claim, we are persuaded the Examiner has erred. Accordingly, we do not sustain the rejection of claim 8 under 35 U.S.C. § 103.

*Claim 10*

Claim 10 depends from claim 1 and recites:

> The method according to claim 1, wherein:
> the computer includes a configuration management system and a configuration management database;

> the asset is a configuration item maintained in the configuration management database; and
> the work order is issued by a change management process or a release management process of the configuration management system.

App. Br. 34 (Claims Appendix). In rejecting claim 10, the Examiner cites to Ratcliff ¶¶ 17, 24–26. Final Act. 9; Ans. 13. Appellants argue paragraph 17 merely describes the use of a database, and provides no teaching of a "configuration management database." Reply Br. 17. Appellants further contend the cited portions of Ratcliff do not teach or suggest a work order that is "issued by a change management process or a release management process." *Id.* According to Appellants, Ratcliff "describes that 'access rights' are stored in a conventional database." *Id.* We agree with Appellants. The Examiner does not identify anything in Ratcliff that corresponds to the recited work order "is issued by a change management process or a release management process." Accordingly, we are persuaded the Examiner erred in rejecting claim 10, and we do not sustain the rejection under 35 U.S.C. § 103.

### *Independent Claim 11*

Appellants argue separately for patentability of independent claim 11. Although the Examiner rejected claim 11 as being substantively the same as claim 1, Appellants argue claim 11 includes limitations that differ in scope, and the Examiner failed to address the differences in those limitations. App. Br. 27–28; Reply Br. 18.

Claim 11 recites:

> A method of processing by a computer to manage an access right to at least one asset associated with at least one digital work order, the method comprising steps executed by the computer of:
>
> at a scheduled start time for a work order to be executed, or in response to reception of a report indicating a start of work for the work order to be executed or a report indicating a completion of work for a preceding work order to the work order to be executed:
>
> > loading into a memory of the computer a security policy associated with the work order to be executed or an asset associated with the work order to be executed, and
> >
> > starting to monitor a location of a moving object present around the asset; and
>
> generating an event for managing the moving object in response to a fact that the loaded security policy is violated by an elapsed time at the location of the moving object that was obtained by the monitoring.

App. Br. 34 (Claims Appendix).

Appellants contend the Examiner has not shown that the cited combination teaches "starting to monitor *a location of a moving object* present around the asset." *Id.* at. 27–28. Appellants argue the Examiner's collective findings addressing claim 1 and claim 11 concurrently fail to address the "moving object" aspect of claim 11. Appellants further contend the "generating" step of claim 11 includes the requirement that "the loaded security policy is violated by an elapsed time at the location of the moving object," another feature not addressed by the Examiner's findings.

We are not persuaded by Appellants' arguments because they do not adequately explain the deficiencies in the Examiner's findings. As we discussed above in connection with claim 1, Ratcliff teaches a security policy that is based on the location of an employee such that if the employee is not at the correct building (i.e., location) during their correct work hours, an access right is not granted to the employee. Ratcliff ¶ 26 ("access rights . . . limited to a period of time surrounding their assigned shift . . . and the section of Building A in which their assigned production operates"). Ratcliff teaches that access to locations may be provided by "keys, codes, biometric, or other devices." Ratcliff ¶ 23.

As such, a person of ordinary skill in the art would have appreciated that enforcement of the location policy would have entailed generating an event such as disabling or electronically modifying an access card, keycard, or biometric device associated with the employee to prevent them from entering a location in violation of the security policy. The location of the Ratcliff's access card (the recited "object") carried by an employee (the recited "present around the asset") would have been monitored at least to detect its proximity to a keypad associated with the facility. As such, we agree with the Examiner that Ratcliff teaches, or least suggests, "starting to monitor a location of a moving object present around the asset," as recited in claim 11.

We also are not persuaded Ratcliff is deficient with respect to the "generating an event" step in claim 11. Ratcliff teaches that the access granted to an employee hinges on both a location (their assigned work facility) and a time (their assigned work hours). Thus, if an employee stays at their work location beyond their assigned work hours, they violate Ratcliff's security policy, and their access card is deactivated. The deactivation of the access card is a generated "event" within the meaning of Appellants' claims. Accordingly, we are not persuaded the Examiner erred in rejecting claim 11, and we sustain the rejection under 35 U.S.C. § 103.

*Claim 13*

Claim 13 depends from claim 11 and recites the limitation "in response to the generation of the event, locking an access control device associated with an access to the asset associated with the work order already started." App. Br. 35 (Claims Appendix). The Examiner relies on Official Notice in rejecting claim 13 (Final Act. 7), and further states "the rejection of Claim 13 is proper for reasons given above with respect to Claim 11 (of which Claim 13 depends upon)." Ans. 14. We agree with Appellants that these findings are insufficient to establish unpatentability with respect to claim 13. Accordingly, we do not sustain this rejection.

*Remaining Claims*

Claims 12 and 18 depend from claim 11 and are otherwise identical to claims 2 and 7. Because we sustain the rejections of claims 2, 6 and 7, we also sustain the rejections of claims 12, 17 and 18. Claims 14–16, 19, and 21 depend from claim 11 and are otherwise identical to claims 3–5, 8, and 10. Because we do not sustain the rejections of claims 3–5, 8, and 10 we also do not sustain the rejections of claims 14–16, 19, and 21. Appellants do not present separate arguments for patentability of claims 9 and 20. As such, they fall with their respective independent claims.

## DECISION

We affirm the Examiner's rejection of claims 1–21 under 35 U.S.C. § 101.

We affirm the Examiner's rejection of claims 1, 2, 6, 7, 9, 11, 12, 18, and 20 under 35 U.S.C. § 103.

We reverse the Examiner's rejection of claims 3–5, 8, 10, 13–17, 19, and 21 under 35 U.S.C. § 103.

No time period for taking any subsequent action in connection with this appeal may be extended under 37 C.F.R. § 1.136(a). *See* 37 C.F.R. § 1.136(a)(1)(iv).

AFFIRMED