BoxInterferences@uspto.gov
Tel: 571-272-4683 Entered: March 31, 2015

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

Alarm.com
Junior Party
(US 8,350,694 B1)
(Inventors: Stephen Scott Trundle & Alison Jane Slavin)

v.

iControl Networks, Inc.
Senior Party
(Application No. 13/311,365)
(Inventors: Paul J. Dawes, Jim Fulker, Carolyn Wales, Reza Raji, and Gerald Gutt)

Patent Interference 106,001 (HHB)
(Technology Center 2400)

Before DEBORAH KATZ, JOHN G. NEW, and HUNG H. BUI, *Administrative Patent Judges.*

BUI, *Administrative Patent Judge*.

DECISION ON MOTIONS – 37 C.F.R. §41.125(a)

I. INTRODUCTION

Pending before us are the following substantive motions:

(1) Alarm.com Motion 1 (Paper 66) seeks entry of judgment of no interference-in-fact between Alarm.com's involved patent 8,350,694 ("the '694 patent") and iControl's involved application 13/311,365 ("the '365 application").

- iControl Opposition 1 (Paper 144).
- Alarm.com Reply 1 (Paper 174).

(2) Alarm.com Motion 2 (Paper 67) seeks entry of judgment against Claims 62, 68, and 74 of iControl's involved application 13/311,365 based on alleged lack of written description under 35 U.S.C. § 112, first paragraph.

- iControl Opposition 2 (Paper 145).
- Alarm.com Reply 2 (Paper 175).

(3) Alarm.com Motion 3 (Paper 68) seeks to designate Claims 2, 7, 13, 22, 27, 33, 42, 47, and 53 of iControl's involved application 13/311,365 as not corresponding to the count.

- iControl Opposition 3 (Paper 146).
- Alarm did not file a reply.

(4) iControl Motion 1 (Paper 27) seeks entry of judgment against all claims of Alarm.com's involved patent 8,350,694 based on an alleged lack of patentability under 35 U.S.C. § 102 and § 103.

- Alarm.com Opposition 1 (Paper 144).
- iControl did not file a reply.

An oral hearing was conducted on February 26, 2015. Both the Junior Party (Alarm.com) and the Senior Party (iControl Networks) presented their arguments

in support of their motions, oppositions and replies. A transcript of the oral hearing was made of record. Paper 198.

After a review of all motions, oppositions and replies, we enter decisions on the following: (1) Alarm.com Motion 2 (Paper 67) for finding adequate written description under 35 U.S.C. § 112, first paragraph; (2) Alarm.com Motion 1 (Paper 66) for finding interference-in-fact; and (3) Alarm.com Motion 3 (Paper 68) for designating Claims 2, 7, 13, 22, 33, 42, 47, and 53 as corresponding to the Count. 37 C.F.R. § 41.125(a). For the reasons discussed below, all three motions from Junior Party Alarm.com, *i.e.*, Alarm.com Motion 2 (Paper 67), Alarm.com Motion 1 (Paper 66), and Alarm.com Motion 3 (Paper 68) are *denied*. As a result, we need not reach iControl Motion 1 (Paper 27) because Junior Party Alarm.com does not allege a date of invention prior to the earliest date accorded to iControl (March 16, 2005 – Paper 1) and does not contest priority (Paper 193, p. 3). Therefore, iControl Motion 1 (Paper 27) is *dismissed* as moot.

II. BACKGROUND

Senior Party iControl requested an interference between: (1) Claims 62–79 of iControl ’365 application, and (2) Claims 1–7, 10, 13, 21–27, 30, 33, 41–47, 50 and 53 of Alarm.com ’694 patent. Interference Request (Ex. 2003, pp. 2–6). 37 C.F.R. § 41.202(a).

The interfering subject matter is directed to a security system designed to permit users to remotely stay connected to their premises (e.g., home) and to remotely access, monitor and control operations of the security system using a mobile device having multiple applications to perform operations of the security system. Ex. 2001, Fig. 1; Ex. 1042, 11:8–22, Figs. 1–2.

The interfering subject matter is represented by a single Count 1, which is Alarm.com Claim 1 or iControl Claim 62.

Claim 1 of the ’694 patent (Junior Party Alarm.com) is reproduced below:

1. A system for monitoring a property, the system comprising:

a monitoring system that is configured to monitor a property and includes one or more sensors that are installed at the property and that are configured to sense attributes of the property;

a native mobile device monitoring application loaded onto a mobile device that is provided separately from the monitoring system by a company that is different than a company that provides the monitoring system, the native mobile device monitoring application including instructions that, when executed by the mobile device, cause the mobile device to perform operations comprising:

performing a synchronization process to synchronize the native mobile device monitoring application with the monitoring system that is configured to monitor the property;

based on the synchronization, receiving one or more data communications descriptive of sensor events detected by the monitoring system at the property;

causing display, on a display device of the mobile device, of a status interface area that includes status information related to the monitoring system based on the received one or more data communications;

causing display, on the display device of the mobile device, of a control interface area that enables a user to provide user input to control the monitoring system;

receiving user input defining a control operation for the monitoring system based on the control interface area; and

> based on the received user input and the synchronization, sending one or more control communications that cause the monitoring system to perform the control operation defined by the received user input.

Paper 11, p. 3 (emphasis added).

Claim 62 of the '365 application (Senior Party iControl) is substantially identical to Claim 1 of the '694 patent (Junior Party Alarm.com), except that: (1) generic "applications" are included in a mobile device instead of "*a native mobile device monitoring application*" and (2) operations performed by the mobile device include "performing a synchronization to *associate* the mobile device with the monitoring system" instead of "performing a synchronization process to *synchronize* the native mobile device application with the monitoring system" as recited in claim 1 of the '694 patent. For example, the relevant portion of claim 62 of iControl '365 application is reproduced below:

> a mobile device that is provided separately from the monitoring system by a company that is different than a company that provides the monitoring system, the mobile device including *applications* that, when run on the mobile device, perform operations comprising:
>
> > performing a synchronization to *associate* the mobile device with the monitoring system …

Paper 8, p. 1 (emphasis added). Alarm.com Claims 1–7, 10, 13, 21–27, 30, 33, 41–47, 50, and 53 (Paper 11; Ex. 1002), as well as all iControl Claims 62–79 (Paper 8; Ex. 2001) have been designated as corresponding to Count 1. Paper 1, pp. 4–5.

With respect to Count 1, the parties have been accorded an earlier constructive reduction to practice date (*i.e.*, benefit for the purpose of priority) of:

Earliest Alarm.com date:	18 May 2010.
Earliest iControl date:	16 March 2005.

In particular, iControl's involved application 13/311,365 has been accorded the following benefit: (1) Application 12/197,895 filed August 25, 2008, now issued as US 8,073,931; (2) Application 12/189,757 filed August 11, 2008, now issued as US 8,473,619; (3) Application 12/019,554 filed January 24, 2008, now issued as US 7,911,341; (4) Application 12/019,568 filed January 24, 2008 (still pending before the PTO); (5) Application 11/761,745 filed June 12, 2007, now issued as US 8,635,350; (6) Application 11/761,718 filed June 12, 2007, now issued as US 7,711,796; (7) Application 11/761,745 filed June 12, 2007, now issued as US 8,635,350; and (8) Application 11/084,232 filed March 16, 2005, now issued as US 8,335,842.

Senior Party iControl filed its Priority Statement (Paper 22) on July 1, 2014 but no such statement was filed by Junior Party Alarm.com. Alarm.com does not allege a date of invention prior to the earliest date accorded to iControl (16 March 2005), and has not contested the March 16, 2005 benefit date accorded to iControl. Paper 193, p. 3. Accordingly, there was no need to authorize motions based on priority. *Id.*

Assuming that Alarm.com does not prevail on its motions, iControl prevails on the issue of priority and all of Alarm.com claims designated as corresponding to the count would be unpatentable.

A. Witnesses

Alarm.com relies on the testimony of Dr. Sam Malek:

(1) First Declaration of Sam Malek, Ph.D., in support of Alarm.com's Request for an Interference. Ex. 2004 (Sam Malek CV), Ex. 2041.

(2) Second Declaration of Sam Malek, Ph.D., in support of Alarm.com Motion 1 (Paper 66), Alarm.com Motion 2 (Paper 67), and Alarm.com Motion 3 (Paper 68); Ex. 2040 (Sam Malek CV), Ex. 2041.

(3) Third Declaration of Sam Malek, Ph.D., in support of Alarm.com Opposition 1 (Paper 142), Ex. 2052.

iControl relies on the testimony of Joe Tipton Cole:

(1) First Declaration of Joe Tipton Cole in support of iControl Motion 1 (Paper 27); Ex. 1003 (J. Tipton Cole CV), Ex. 1002.

(2) Second Declaration of Joe Tipton Cole in support of iControl Opposition 1 (Paper 144), iControl Opposition 2 (Paper 145), and iControl Opposition 3 (Paper 146); Ex. 1043.

1. Dr. Malek

Dr. Malek is an Associate Professor and Director of Software Design and Analysis Laboratory at George Mason University, and has a Ph.D. degree in Computer Science as well as a M.S. degree in Computer Science from University of Southern California. Ex. 2040, ¶¶ 2, 5, 6; Ex. 2041.

Dr. Malek has over 15 years of experience in research pertaining to software engineering, including software design and architecture, distributed and embedded systems, software design and architecture, distributed and embedded systems, smartphone and mobile computing, internet and web technologies, middleware, service oriented computing, autonomic computing, and software dependability and security. He has published many papers in the same field of software engineering. Ex. 2040, ¶¶ 3–4; Ex. 2041.

Dr. Malek is qualified to express opinions regarding the technology involved in this case.

2. Mr. Cole

Mr. Cole is a principal at Tipton Cole & Company, technical consultant services in the area of computer software and associated devices. Ex. 1003 ¶ 3; Ex. 1002. He has a M.S. degree in Computer Science and a B.A. in Mathematics from the University of Texas. Ex. 1003 ¶ 5. Mr. Cole also has 40 years of experience in software development and, since 2008, technical consulting services involving computer software. Ex. 1002.

Mr. Cole is qualified to express opinions regarding the technology involved in this case.

III. ALARM.COM MOTION 2 (PAPER 67) FOR LACK OF WRITTEN DESCRIPTION

Alarm.com Motion 2 (Paper 67) moves for judgment against Claims 62–79 of iControl's involved application 13/311,365 based on an alleged lack of a written description under 35 U.S.C. § 112, first paragraph. Specifically, Alarm.com contends iControl's involved application does not provide written description support for three limitations:

> (1) "the mobile device including applications that, when run on the mobile device, perform operations comprising: performing a synchronization to associate the mobile device with the monitoring system;"
>
> (2) "based on the synchronization, receiving by the mobile device one or more data communications descriptive of sensor events detected by the monitoring system at the premise;" and
>
> (3) "based on the received user input and the synchronization, sending one or more control communications that cause the

> monitoring system to perform the control operation defined by the received user input"

as recited in independent claims 62, 68, and 74 of iControl's involved application. Paper 67 at 4–18.

B**e**low are our findings of facts regarding the disclosure of iControl's involved application, analysis and conclusions of law regarding written description support for the disputed limitations recited in independent claims 63, 68, and 74 of iControl's involved application.

A. FINDINGS OF FACTS

We make the following findings of facts ("FFs") to resolve issues presented in Alarm.com Motion 2 (Paper 67) and subsequent motions. These FFs, as well as others made elsewhere in the Decision, are supported by at least a preponderance of the evidence on the record. *Ethicon, Inc. v. Quigg*, 849 F.2d 1422, 1427 (Fed. Cir. 1988).

1.

iControl's Involved Application (the '365 Application)

1. iControl '365 application discloses an integrated security system, shown in Fig. 1 and Fig. 2, that integrates broadband and mobile access and control with conventional security systems and premise devices to provide a security network (broadband, cellular/GSM[1], POTS[2] access) that enables an end user client using a mobile device to remotely stay connected to their premises (e.g., home)

[1] GSM is known as "Global System for Mobile Communications," a standard developed by the European Telecommunications Standards Institute (ETSI) to describe protocols for digital cellular networks used by mobile phones. .

[2] PTOS is known as "Plain Ordinary Telephone Service." Ex. 1042, 9:19–20.

and to remotely access, monitor, manage and control operation of the conventional security system, via a network. Ex. 1042, 6:14–22, 7:14–29, Figs. 1–2.

2. iControl's Fig. 1 is reproduced below with additional markings for illustration.

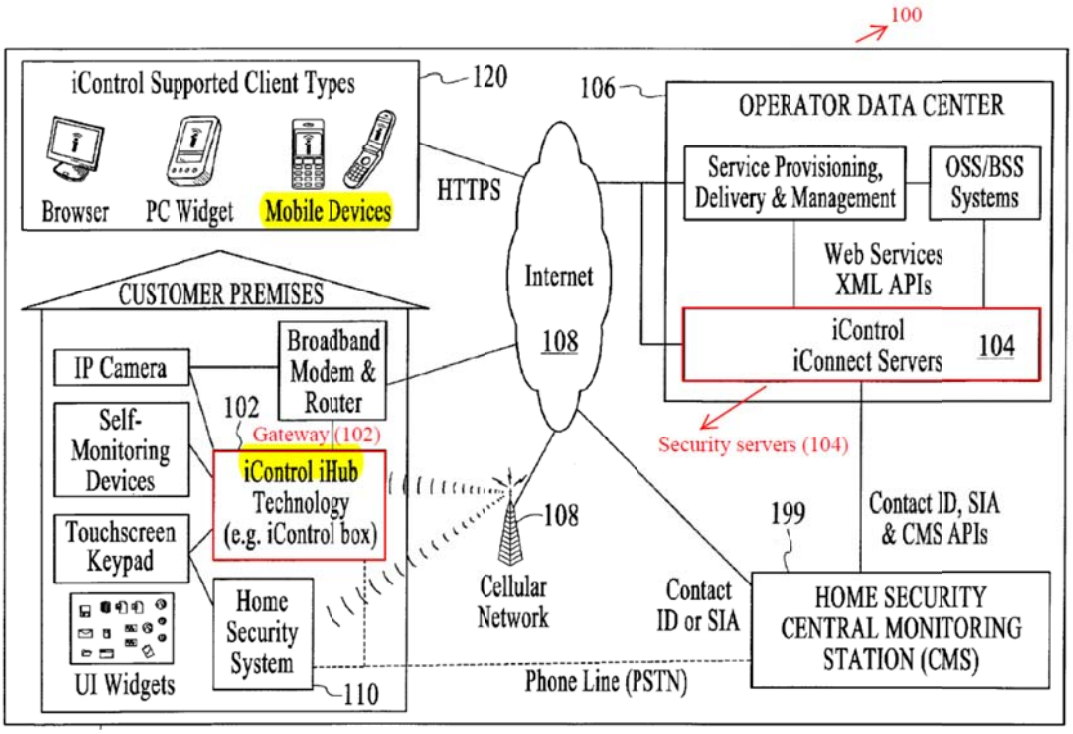


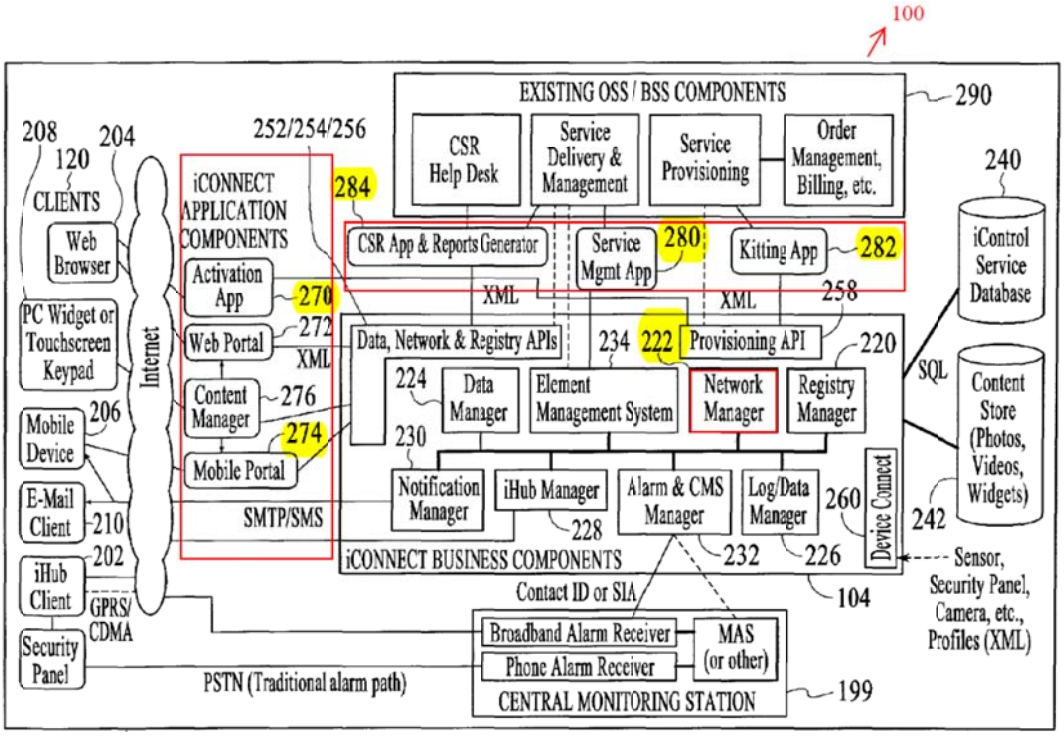
Fig. 1 shows an integrated security system 100 designed to permit an end user client to remotely stay connected to the client's premise and to remotely access, monitor and control operation of the security system using the mobile device.

As shown in iControl's Fig. 1, the integrated security system 100 includes: (1) a gateway (a.k.a "iHub") 102 and (2) security system servers (a.k.a "iConnect servers") 104 coupled to a conventional home security system 110 and associated devices. The gateway 102 is located at a customer's premise (home or business) and used to: (1) connect, manage, and control the security system 110 equipped with a variety of home security and self-monitoring devices (e.g., sensors, controllers, cameras, etc.), and (2) communicate with the security servers 104

located at a service provider's data center 106, via a network 108 (e.g., cellular network, Internet, etc.). The combination of the gateway 102 and the security system servers 104 enables an end user client 120 using a mobile device 206 to remotely stay connected to the premise (home or business) and to remotely access, monitor, manage and control operation of the security system 110 and associated security and self-monitoring devices, via the network 108 (e.g., cellular network, Internet, etc.). *Id*. at 11:8–22.

3. iControl's Fig. 2 provides more detail of an integrated security system 100 where a service is delivered by the security system (iConnect) servers 104 running a variety of applications (software components) that communicate with a variety of client types including a mobile device 206. *Id*. at 12:8–12.

4. iControl's Fig. 2 is reproduced below with additional markings for illustration.



iControl's Fig. 2 shows more detail of the integrated security system services provided by the security system servers 104 at the operator data center 106.

As shown in iControl's Fig. 2, the security system (iConnect) servers 104 support numerous types of software components (applications) designed for different purposes, including, for example:

> (1) Business Components (e.g., a Registry Manager 220, a Network Manager 222, a Data Manager 224, a Log/Data Manager 226, an iHub Manager 228, a Notification Manager 230, an Alarm/CMS Manager 232, and an Element Management System (EMS) 234) designed *to manage all of the home security and self-monitoring devices at the premise*;
>
> (2) End-User Application Components (e.g., an Activation Application 270, a Web Portal Application 272, a Mobile Portal 274, and a Manager Application Component 276) designed *to allow the end users to access the Business Components, via APIs (Java APIs or XML APIs), and control all of the home security and self-monitoring devices at the premise*; and
>
> (3) Service Management Application Components (e.g., a Service Management Application 280, a Kitting Application 282, and a CSR Application and Report Generator 284) *responsible for overall management of the service*.

Id. at 13:21–28, 14:15–19:2 (emphases added).

5. For purposes of this interference, these End-User Application Components (e.g., the Activation Application 270, the Web Portal Application 272, the Mobile Portal 274 and the Content Manager Application Component 276) run on the security system servers 104; however, these application components generate CSS-based HTML/JavaScripts that are delivered to end user clients (mobile devices) where the CSS-based HTML/JavaScripts run as "applications" that provide user interfaces for the end user client 120 using a mobile device 206 to access and control the security system 100. *Id*. at 17:6–18:11.

6. For example:

> An iControl Activation Application 270 that delivers the first application that a user [at mobile device] sees when they set up the integrated security system. This wizard-based web browser application [at mobile device] *securely* ***associates*** *a new user with a purchased gateway and the other devices* included with it as a kit (if any). It primarily uses functionality published by the Provisioning API.
>
> An iControl Web Portal Application 272 runs on PC browsers and delivers the web-based interface to the integrated security system service. This application allows users to manage their networks (e.g. add devices and create automations) as well as to view/change device states, and manage pictures and videos. Because of the wide scope of capabilities of this application, it uses three different Business Component APIs that include the Registry Manager API, Network Manager API, and Data Manager API, but the embodiment is not so limited.
>
> An iControl Mobile Portal 274 is a small-footprint *web-based interface that runs on mobile phones* and PDAs. This interface is optimized for remote viewing of device states and pictures/videos rather than network management."

Id. at 17:16–27 (emphases added).

7. In turn, the "Kitting Application 282 is used by employees performing service provisioning tasks. This application allows *home security and self-monitoring devices to be* ***associated*** *with gateways* [102] during the warehouse kitting process." *Id.* at 18:25–27 (emphasis added).

8. Each gateway-enabled device is assigned a unique activation key for activation with the security system (iConnect) servers 104 in order to ensure that only valid gateway-enabled devices can be activated for use with the specific instance of iConnect servers 104 in use. *Id*. at 20:18–21.

9. The Network Manager 222 then handles the creation, modification, deletion and configuration of all devices on the integrated security system network (e.g., controllers, sensors, cameras, etc.) as well as the creation of automations, schedules and notification rules associated with those devices. *Id.* at 14:29–15:2. In particular, "The Network manager ***synchronizes*** with the gateway [102], the advanced touchscreen, and the subscriber database." *Id.* at 32:4–7 (emphasis added).

10. After the gateway 102 has completed the discovery and learning of all devices on the integrated security system network and has been integrated as a virtual control device, the security system and associated devices (e.g., sensors, controllers, cameras, etc.) become operational and are presented as accessible devices to a potential plurality of user interface subsystems at a mobile device 206. *Id.* at 32:4–7, 68:16–30, 69:5–18.

11. The gateway 102 then transmits messages comprising event data of the security system and associated devices (e.g., sensors, controllers, cameras, etc.) to the end user client 102 using a mobile device 206, via the network (Internet) 108. *Id.* at 32:4–7, 68:16–30, 69:12–16.

12. According to iControl, user interface subsystems (*i.e.*, monitoring and control applications) are also used to allow an end user client 120 at a mobile device 206 to monitor, manage, and control the security system and associated devices (e.g., sensors, controllers, cameras, etc.), via a Web browser or equivalent application running on the mobile device 206. *Id.* at 45:11–13.

> In an embodiment of the system, *a user interface subsystem is an HTML/XML/Javascript/Java/AJAX/Flash presentation of a monitoring and control application*, enabling users to view the state of all sensors and controllers in the extant security system from a web browser or equivalent operating on a … *mobile phone*, or other consumer device.

> In another illustrative embodiment of the system described herein, *a user interface subsystem is an HTML/XML/Javascript/Java/AJAX presentation of a monitoring and control application*, enabling users to combine the monitoring and control of the extant security system and sensors with the monitoring and control of non-security devices including but not limited to IP cameras, touchscreens, lighting controls, door locking mechanisms.

Id. at 45:13–26 (emphases added).

13. The Notification Manager 230 is responsible for communicating with the end user client 120 at the mobile device 206, via the network (Internet) 108, and sending all notifications to the end user client 120 at the mobile device 206, via email and text messages that are displayed by email and text applications running on the mobile device 206. *Id.* at 15:18–20, 32:4–7.

14. In view of FF 3–13, iControl describes multiple applications that perform operations when run on a mobile device 206 (via a web browser), including: (1) those applications that are resident at the mobile device 206 such as Web browsers, email SMS, or text applications; and (2) those applications that are resident at the security system servers 104 (a.k.a., Web servers) such as user interface subsystems (*i.e.*, monitoring and control applications) and End-User Application Components (*i.e.*, Activation Application 270, Web Portal Application 272, and Mobile Portal 274) but are delivered or downloaded to the mobile device 206 from the security system servers 104 (a.k.a., Web servers) in the form of CSS-based HTML/JavaScripts where the CSS-based HTML/JavaScripts run as "applications" that provide user interfaces for the end user client 120 at the mobile device 206 to access and control the security system 100.

15. iControl further describes these end user clients 120 can be:

> *Custom-built clients* (not shown) that access the iConnect web services XML API to interact with users' home security and self-monitoring information in new and unique ways. Such *clients could include new types* of mobile devices, or complex applications where integrated security system content is integrated into a broader set of application features.

Id. at 13:12–16 (emphases added).

16. iControl also describes that automation devices (camera, lamp modules, thermostats, etc.) can be added *enabling an end user* [client] to remotely see live video and/or pictures and *control home devices via a mobile device*. *Id*. at 6:22–24 (emphasis added). In addition, the mobile device 206 can also be used to view the system status and *perform operations on associated devices* (e.g., turning on a lamp, arming a security panel, etc.). *Id*. at 12:26–29 (emphasis added).

B. ANALYSIS

1.

As an initial matter, we note that Claims 62–79 of iControl's involved application were not copied from Alarm.com's '694 patent and, as such, iControl Claims 62–79 must be interpreted in the context of the specification of iControl's disclosure for purposes of determining compliance with the written description requirement of 35 U.S.C. § 112, first paragraph. *See Agilent Tech., Inc. v. Affymetrics, Inc.*, 567 F.3d 1366, 1375 (Fed. Cir. 2009). Moreover, the only appropriate specification for the determination of adequate written descriptive support is the specification in which the involved claims form a part, iControl's involved application. *See Reiffin v. Microsoft Corp.*, 214 F.3d 1342, 1346 (Fed. Cir. 2000).

2.

Whether the descriptive portion of a specification contains a written description of claimed subject matter is an issue of fact. *Chen v. Bouchard*, 347 F.3d 1299, 1304 (Fed. Cir. 2003); *In re Alton*, 76 F.3d 1168, 1171-72 (Fed. Cir. 1996).

In order to satisfy the written description requirement under 35 U.S.C. § 112, first paragraph, the specification must convey with reasonable clarity to those of ordinary skill in the art that as of the filing date of the application the inventor disclosed the claimed invention. *Vas-Cath Inc. v. Mahurkar*, 935 F.2d 1555, 1563-64 (Fed. Cir. 1991); *see also Pandrol USA, LP v. Airboss Ry. Products, Inc.*, 424 F.3d 1161, 1165 (Fed. Cir. 2005). The purpose of the written description requirement is to prevent applicants from later asserting that they invented that which they did not. *Amgen Inc. v. Hoechst Marion Roussel Inc.*, 314 F.3d 1313, 1330 (Fed. Cir. 2003). However, an applicant does not have to utilize any particular form of disclosure to describe the subject matter claimed, but "the description must clearly allow persons of ordinary skill in the art to recognize that [the applicant] invented what is claimed." *In re Gosteli*, 872 F.2d 1008, 1012 (Fed. Cir. 1989). Likewise, the language in the written description does not have to be in the exact same words, *in ipsis verbis*, as the language at issue in the corresponding claim. *In re Wertheim*, 541 F.2d 257, 265 (CCPA 1976); *In re Lukach*, 442 F.2d 967, 969 (CCPA 1971).

3.

As the moving party, Alarm.com bears the burden of proof to demonstrate entitlement to the relief requested. 37 C.F.R. § 41.121(b). To be sufficient, a

motion must provide a showing, supported with appropriate evidence, such that, if unrebutted, it would justify the relief sought. 37 C.F.R. § 41.208(b). The applicable standard of proof is by a preponderance of the evidence. *See, e.g.*, *Bilstad v. Wakalopulos*, 386 F.3d 1116, 1129 (Fed. Cir. 2004); *Bruning v. Hirose*, 161 F.3d 681, 685 (Fed. Cir. 1998).

4.

Alarm.com argues that three limitations of iControl Claims 62–78 lack written description support. Paper 67 at 4–18.

> (1) First Limitation: "the mobile device including applications that, when run on the mobile device, perform operations comprising: performing a synchronization to associate the mobile device with the monitoring system."

iControl's first limitation allegedly not described by iControl's written description contains two parts: (A) the mobile device includes multiple applications that perform operations when run on the mobile device, and (B) such operations include "performing a synchronization to associate the mobile device with the monitoring system." Paper 8, p. 1; Ex. 2001, Claim 62.

With respect to the first part, Alarm.com acknowledges the End-User Application Components such as an iControl Activation Application 270 and a Kitting Application 282 as disclosed by iControl constitute "multiple applications" that perform operations. Paper 67 at 6. However, Alarm.com argues such applications are not included on a mobile device; rather, these applications are web applications that reside on a remote server, *i.e.*, security system servers 104, shown in Figs. 1–2 of iControl's disclosure, and are then delivered to a mobile device 206 for execution. *Id*. at 6–8.

Alarm.com relies on the testimony of Dr. Sam Malek to support its no written description argument. Ex. 2003 and Ex. 2040. In particular, Dr. Malek testified that:

> [1] Each of these applications [*i.e.*, an iControl Activation Application 270 and a Kitting Application 282] is defined as "End-User Application Components [that] generate CSS-based HTML/JavaScript that is displayed on the target client." *Applications that generate CSS-based HTML/JavaScript are web applications that are not included on a mobile device*. Rather, web applications are included on a remote web server and content from web applications is displayed by target clients.
>
> [2] There are some major differences between an application included on a mobile device and a mobile web application. *Web applications reside on a remote server and are delivered to a mobile device for execution…. Mobile applications that are included on a mobile device* are also generally more amenable to providing offline functionality, since the application does not depend on access to a remote web server for downloading the HTML/Javascript content. Mobile applications that are included on a mobile device generally provide a more convenient and intuitive experience for the users, as the user interface is consistent with the other applications running on a given platform….
>
> [3] FIG. 2 of the '365 application … clearly shows that the Activation App 270 and the Kitting Application 282 are separated from all clients 120, including mobile device 206, by the Internet and are included on a remote server. Accordingly, *the '365 application does not describe that either the Activation App 270 or the Kitting Application 282 is included on the mobile device 206*, much less that both the Activation App 270 and the Kitting Application 282 are included on the mobile device 206,… which would be required to meet the requirement of claim 62 for multiple applications included on a mobile device that perform operations when run on the mobile device.

Ex. 2040 at ¶¶ 22, 24–25 (emphasis added).

We are cognizant of the differences between: (1) web applications that reside on a remote server and are delivered to a mobile device and run in a mobile device's web browser, such as those disclosed by iControl's disclosure, and (2) client mobile applications or "native applications" that are included on a mobile device, as Alarm.com argues. However, we find Alarm.com's arguments misplaced and unpersuasive. Nor do we find Dr. Malek's testimony persuasive on this point.

Pending claims in interference proceedings are given their broadest reasonable construction in a manner consistent with *Agilent, i.e.*, in light of iControl's disclosure. Claim terms are also accorded their ordinary and accustomed meaning as would be understood by one of ordinary skill in the art after reading the entire patent, *i.e.*, iControl's disclosure. *Phillips v. AWH Corp.*, 415 F.3d 1303, 1323 (Fed. Cir. 2005) (*en banc*).

At the outset, we note that iControl Claim 62 simply recites "a mobile device including applications that, when run on the mobile device, perform operations." Paper 7, Ex. 2001. iControl Claim 62 does not require these "applications" be either "web applications" or "client mobile [or native] applications." Nor does iControl Claim 62 requires these "applications" be embedded on a mobile device. Alarm.com argues the plain language of iControl Claim 62 simply requires some "applications" that run on a mobile device, regardless of whether those applications are: (1) web applications that reside on remote servers, or (2) client mobile applications or "native applications" that reside on a mobile device. iControl Opposition 2 (Paper 145), 8:16–17. Thus, Alarm.com's argument that iControl's disclosure does not describe applications included on a mobile device is insufficient on its face. Alarm.com's bases its attack on Claim 62 on an overly narrow construction of "applications."

Even if the term "applications" in iControl Claim 62 is as broad as iControl suggests, we agree with iControl that applications included on a mobile device are described in its disclosure. As explained by iControl, when the CSS-based HTML/JavaScripts are generated by the End-User Application Components such as, for example, the Activation Application 270, the Web Portal Application 272, the Mobile Portal 274 and the Content Manager Application Component 276, as shown in Fig. 2 of iControl's disclosure, and are delivered or downloaded to a mobile device 206, those CSS-based HTML/JavaScripts constitute "applications" and run as "applications" on a mobile device 206, as shown in iControl's Fig. 2, that provide user interfaces for an end user client at the mobile device 206 to access and control the security system 100. Paper 145 at 10:1–4 and 7–15 (citing Ex. 1042 at 17:6–18:11); *see also* Figs. 1–2; and FF 4–5.

As further explained by iControl, iControl's disclosure ("the '365 application") also describes several additional types of "applications" that also perform operations when run on a mobile device 206, such as web browsers and mobile web browsers, both of which run client-side Javascript applications, widgets, email and text messaging applications. Paper 145, 8:18–21 (citing Ex. 1042, 12:13–13:16); *see also* FF 12–14. These client mobile device applications are also coupled to End-User Application Components running on security system servers 104. *Id*. at 10:7–15; *see also* Ex. 1042, 17:14–18:11, 15:12–20, and Figs. 1–2. Other client mobile device applications are also described by the '365 application as: (1) user interface subsystems (*i.e.*, monitoring and control applications), and (2) "A Notification Manager 230 is responsible for sending all notifications to clients via SMS (mobile phone messages), email (via a relay server like an SMTP email server), etc." *Id*. at 11:3–8 (citing Ex. 1042, 15:18–20). SMS, email and browsers are all client mobile device applications, and they are all part

of the written description of iControl's disclosure that shows possession of "the mobile device including applications that, when run on the mobile device, perform [the recited] operations." *Id*. at 9:3–8; FF 12–14.

With respect to the second part, the term "synchronization" is not defined by the '365 application. Nor does Alarm.com proffer a construction of the term "synchronization" in the context of "to associate the mobile device with the monitoring system." Instead, Alarm.com lodges an attack of iControl's interference request (Ex. 2003) for failing to demonstrate adequate written description for "performing a synchronization to associate a mobile device with a monitoring system" as recited in iControl's claims, based on: (1) what Alarm.com characterizes as "disjointed" and "unrelated portions" of the '365 application and (2) the testimony from Dr. Malek (Ex. 2040) confirming that none of these "disjointed" and "unrelated portions" of the '365 application describe the disputed limitation. Paper 67 at 5–13 (citing Ex. 2003, Ex. B, p. 3–4; Ex. 2042, ¶¶ 28–31).

For example, Alarm.com acknowledges the iControl Activation Application 270 and the Kitting Application 282 as disclosed by iControl relate to: (1) association of a new user with a gateway and associated devices, and (2) association of home security and self-monitoring devices with gateways. Paper 67 at 9–10 (citing Ex. 2003, Ex. B, p. 3–4; Ex. 2042, ¶¶ 28–31); *see also* FF 6–7. Nevertheless, Alarm.com argues: (1) associating a user with a gateway does not necessarily require associating a mobile device with the gateway, (2) associating home security and self-monitoring devices with a gateway does not necessary require associating a mobile device with the gateway and, as such, (3) one skilled in the art would not understand an association of "a user with a gateway" or "home security and self-monitoring devices with a gate" as being an association of a mobile device with a monitoring system. *Id*.

Alarm.com also argues: (1) a mere activation of a gateway-enabled device with a server does not convey that the activation includes performance of a synchronization to achieve the activation; (2) synchronization between the Network Manager (a component of a remote server shown in iControl's Fig. 2) and the gateway, the advanced touchscreen, and the subscriber data does not involve or associate a mobile device with a monitoring system; and (3) installation, such as creating a new user account and associating that user account with a security network or system as described by the '365 application does not involve "performing a synchronization to associate a mobile device with a monitoring system." *Id*. at 11–13.

However, Alarm.com's arguments and proffered evidence are predicated on a narrow reading of what Alarm.com characterizes as "disjointed" and "unrelated portions" of the '365 application. As such, we find Alarm.com's arguments unpersuasive. The language in the written description does not have to be in the exact same words as the language in iControl's claims. *In re Wertheim*, 541 F.2d 257, 265 (CCPA 1976). Rather, the description is written to enable a person skilled in the art to recognize that iControl had possession of what is claimed, *i.e.*, "performing a synchronization to associate the mobile device with the monitoring system." *In re Gosteli*, 872 F.2d 1008, 1012 (Fed. Cir. 1989). Neither the term "synchronization" nor "associate" is defined by the '365 application. However, the term "synchronization to associate" is described in the context of the overall process of associating a mobile device [including applications] with a monitoring system in a network environment shown in iControl's Figs. 1–2, that involve several network components, including, for example: End-User Application Components (e.g., the Activation Application 270, the Web Portal Application 272, the Mobile Portal 274 and the Content Manager Application

Component 276), the Network Manager 222, the gateway 102 and user interface subsystems (*i.e.*, monitoring and control applications) in order to allow an end user client at a mobile device to monitor, manage, and control the security system and associated devices. Ex. 1042, 6:14–22, 7:14–18, 11:8–22, 12:8–12, 13:21–28, 14:15–19:2, 32:4–7, 45:13–26, 58:5–8, 68:16–30, 69:5–18; Figs. 1–2, and FF 1–13.

For example, as pointed out by iControl, the '365 application describes:

> "The following End-User Application Components generate CSS-based HTML/JavaScript that is displayed on the target client… The End-User Application Components of an embodiment include…An iControl Activation Application 270 that delivers the first application that a user sees when they set up the integrated security system service. This wizard-based web browser application *securely associates a new user with a purchased gateway* and the other devices included with it as a kit (if any)."

iControl Opposition (Paper 145) at 12:7–16 (citing Ex. 1042, 17:11–19) (emphasis added), FF 5–6. In other words, the web browser application and the CSS-based HTML/JavaScript application (that run on a mobile device 206) associate a user of a mobile device 206 with the gateway 102, shown in iControl's Figs. 1–2.

As explained by iControl, the gateway 102 has already been associated with the monitoring system 110 at the customer's premise (home or office) by one of a few methods: "A Kitting Application 282 is used by employees performing service provisioning tasks. This application allows home security and self-monitoring devices to be associated with gateways during the warehouse kitting process." *Id*. at 12 (citing Ex. 1042, 18:25–27). *See also*, Ex. 1042, FIG. 16; 44:15–45:17; FF 6–8.

> "After the gateway [102] has completed the discovery and learning 1640 of sensors and has been integrated 1650 as a virtual control device in the extant security system, the [security] system

> becomes operational. Thus, the security system [110] and associated sensors are presented 1650 as accessib1e devices to a potential plurality of user interface subsystems."

Id. (citing Ex. 1042, 45:1–5); FF 9–10. The '365 application then describes:

> "a user interface subsystem 1670 enabling a user to monitor, manage, and control the system and associated sensors and security systems. In an embodiment of the system, a user interface subsystem is an HTML/XML/Javascript/Java/AJAX/Flash presentation of a monitoring and control application, enabling users to view the state of all sensors and controllers in the extant security system from a web browser or equivalent operating on a mobile device."

Id. at 11–12 (citing Ex. 1042, 45:11–17); FF 11. That is, a web browser or similar application (along with a CSS-based HTML/JavaScript) running on a user's mobile device 206 is associated with the monitoring system 110, allowing the user to control the monitoring system 110 with the mobile device 206.

According to iControl's expert, Tipton Cole testified:

> "To monitor and control the monitoring system after the initial synchronization, the user enters a username and password on the mobile device 206. "Installer instructs customer on use of the Simon XT, and shows customer how to log into the iControl web and mobile portals. Customer creates a username/password at this time." Ex. 1042, 56:2–4, 58:5–7. That is, for subsequent access to the monitoring system with a mobile device, the user logs into a web browser or equivalent user interface running on the mobile device by entering the username and password, thereby associating the mobile device 206 with the monitoring system."

Id. (citing Ex. 1043 ¶272).

As described throughout the '365 application, an end user client of the mobile device 206 can monitor, manage, and control the system and associated devices, which requires an application on the mobile device 206 to perform a synchronization to associate the mobile device 206 with the monitoring system

110. *See*, *e.g.*, Ex. 1042, 45:11–17. While the association between the mobile device 206 and the monitoring system 110 may involve a few network components such as security system servers 104 and a gateway 102, multiple applications on the mobile device 206 perform a "synchronization to associate the mobile device with the monitoring system." Ex. 1042, 6:14–26.

In this context, we find iControl's response and Mr. Cole's testimony consistent with iControl's disclosure. As such, we find iControl's involved application provides adequate written description for "performing a synchronization to associate a mobile device with a monitoring system" as recited in iControl's claims. We also find the written description in iControl's involved application reasonably conveys to one of ordinary skill in the art that iControl had possession of that limitation.

> (2) Second Limitation: "based on the synchronization, receiving by the mobile device one or more data communications descriptive of sensor events detected by the monitoring system at the premise."

Alarm.com argues because the '365 application fails to provide written description support for "performing a synchronization to associate a mobile device with a monitoring system," the '365 application cannot provide written description support for any operation "based on the synchronization." Paper 67 at 13–14. In particular, Alarm.com acknowledges that the '365 application teaches notifications of sensor events sent to a user at a mobile device 206, via email or text messages after the gateway 102 has completed the discovery and the "system becomes operational." *Id*. at 14 (citing Ex. 1042, 45:1–5, 6:25–26, 13:9–11, 14:10–12). Nevertheless, Alarm.com argues: (1) sensor events or (2) notifications or messages

sent to the user as disclosed by iControl are not based on any synchronization to associate a mobile device with a monitoring device. *Id.* at 15.

We disagree. As iControl argues, Claim 62 simply requires the receiving step follows the synchronization. iControl Opposition (Paper 145) at 15:18-21. The '365 application describes these notifications or communications descriptive of sensor events detected by the monitoring system following the synchronization. *Id.* at 16:7-9 (citing Ex. 1042, 45:11–26); *see also* Ex. 1042, 32:4–7, FF 9–12.

Accordingly, we find iControl's involved application provides adequate written description for "based on the synchronization, receiving by the mobile device one or more data communications descriptive of sensor events detected by the monitoring system at the premise" as recited in iControl's claims. We also find the written description in iControl's involved application reasonably conveys to one of ordinary skill in the art that iControl had possession of that limitation.

> (3) Third Limitation: "based on the received user input and the synchronization, sending one or more control communications that cause the monitoring system to perform the control operation defined by the received user input."

Similarly, Alarm.com argues because the '365 application fails to provide written description support for "performing a synchronization to associate a mobile device with a monitoring system," the '365 application cannot provide written description support for any operation "based on the synchronization" much less "based on the received user input and the synchronization, sending one or more control communications that cause the monitoring system to perform the control operation defined by the received user input." Paper 67 at 13-14. In particular, Alarm.com acknowledges the '365 application teaches the gateway 102 and security system (iConnect) servers 104 that enable an end user to remotely stay

connected to the premise (home or office) and to remotely access and control operation of the security system 110 and associated devices, via the network 108. *Id*. at 16 (citing Ex. 1042, 11:12–19). Nevertheless, Alarm.com argues such communications do not describe: "sending one or more control communications that cause the monitoring system to perform the control operation defined by the received user input." *Id*. at 18.

We disagree. Rather, we agree with iControl that the disclosure of the '365 application provides that when an end user client at a mobile device 206 is permitted to monitor, manage, and control a security system 110 and associated devices (e.g., sensors, controllers, cameras, etc.), via a web browser or equivalent application (along with a CSS-based HTML/JavaScript) running on the mobile device 206, control communications are sent to the monitoring system that cause the monitoring system to perform the control operation defined by the received user input in the manner recited by iControl claims. iControl Opposition (Paper 145) at 17:13-18:2 (citing Ex. 1042, 11:8–22, 12:26–29); *see also* Ex. 1042, 11:8–22, FF 11, 16.

As such, we find iControl's involved application provides adequate written description for "based on the received user input and the synchronization, sending one or more control communications that cause the monitoring system to perform the control operation defined by the received user input" as recited in iControl's claims. We also find the written description in iControl's involved application reasonably conveys to one of ordinary skill in the art that iControl had possession of that limitation.

For the foregoing reasons, we conclude that Alarm.com has not satisfied its burden of establishing that the written description portion of iControl does not

describe the disputed limitations within the meaning of iControl Claims 62–79. Therefore, Alarm.com Motion 2 (Paper 67) is *denied*.

IV. ALARM.COM MOTION 1 (PAPER 66) FOR NO INTERFERENCE-IN-FACT

Alarm.com Motion 1 (Paper 66) seeks entry of judgment for no interference-in-fact between the subject matter of Alarm.com's claims and the subject matter of iControl's claims. Paper 67, pp. 1–17.

Alarm.com contends that (1) the subject matter of its claims (*i.e.*, independent claims 1, 21, and 41) differ in scope from iControl's claims (*i.e.*, independent claims 62, 67, and 74), and (2) the subject matter of iControl's claims does not anticipate or render obvious the subject matter of Alarm.com's claims. *Id*. In particular, relevant portions of Alarm.com's claims and iControl's claims are reproduced below:

iControl Claims 62, 67, and 74 recite:

> "a mobile device that is provided separately from the monitoring system by a company that is different than a company that provides the monitoring system, the mobile device including *applications that, when run on the mobile device, perform operations* comprising:
>
> performing a *synchronization to associate* the mobile device with the monitoring system."

Ex. 2003, Claims 62, 67, and 74 (emphasis added).

In contrast, Alarm.com's claims recite:

> "*a native mobile device monitoring application* loaded onto a mobile device that is provided separately from the monitoring system by a company that is different than a company that provides the monitoring system, *the native mobile device monitoring application including instructions that, when executed by the mobile device, cause the mobile device to perform operations* comprising:

> performing a *synchronization process to synchronize* the native mobile device monitoring application with the monitoring system that is configured to monitor the property."

Ex. 2011, Claim 1 (emphasis added).

Alarm.com identifies the differences between Alarm.com's claims and iControl's claims as: (1) the specific use of "*a native mobile device monitoring application*" instead of generic "applications" included in a mobile device, and (2) operations performed by the mobile device include "performing a synchronization process to *synchronize* the native mobile device application with the monitoring system" instead of "performing a synchronization to *associate* the mobile device with the monitoring system" as recited by iControl's claims. Paper 66, p. 10.

As evidence of the non-obviousness of Alarm.com's claims in view of iControl's claims and the state of the art, Alarm.com submits: (1) a Declaration from the inventor of the '694 patent, Alison Slavin, to confirm that she is unaware of any prior art or other reasons that account for the differences between Alarm.com's claims and iControl's claims and the state of the art (Ex. 2005); (2) a Declaration from industry expert, Dr. Malek, to confirm that he is unaware of any prior art or other reasons that would account for the differences between Alarm.com's claims and iControl's claims and the state of the art (Ex. 2004); and (3) the prosecution history of U.S. Patent Application No. 13/735,193 (hereinafter "the '193 application"), a continuation application from the '694 patent, to confirm that the differences between Alarm.com's claims and iControl's claims and the state of the art are not obvious (Ex. 2008). *Id*.

Below are our findings of facts regarding the relevant prior art, the disclosure of Alarm.com '694 application, analysis and conclusions of law regarding patentability of the contested claims of Alarm.com '694 application.

A. ADDITIONAL FINDINGS OF FACTS

1.

State of the Art

17. Prior to the filing date (May 18, 2010) of Alarm.com '694 patent, the use of mobile phones as remote control devices to interact with, control, and respond to home security systems was known. *See* Ex. 1023[3] ("Remote Control Apps for the iPhone"); Ex. 1024[4] ("Psiloc Infrared Remote Control (Symbian)"; Ex. 1030[5] ("iPhone Home Security App"); and Ex. 1031[6] ("Mobile Control System For Location Based Alarm Activation").

18. Prior to the filing date of Alarm.com '694 patent, home security systems accessed using web browsers using JavaScript and/or HTML were also

---

[3] The article "Remote Control Apps for the iPhone" was posted on June 25, 2009 at http://mac.appstorm.net/roundups/iphone-roundups/9-remotecontrol-apps-for-iphone/ (Exhibit 1023).

[4] The article "Psiloc Infrared Remote Control (Symbian)" was posted on August 28, 2007 at http://download.cnet.com/Psiloc-Infrared-Remote-Control-Symbian/3000-2064_4-10730991.html (Exhibit 1024).

[5] The article "iPhone Home Security App" was posted on August 27, 2009 at http://homesecuritysource.wordpress.com/2009/08/27/iphone-home-security-app/ (Exhibit 1030).

[6] The article "Mobile Control System for Location Based Alarm Activation" was available on June 16, 2008 by Jan Magne Tjensvold, Master's thesis, Dept. of Electrical Engineering and Computer Science, University of Stavanger, Norway (http://brage.bibsys.no/xmlui/handle/11250/181677) (Exhibit 1031).

known in the art. *See* Ex. 1032[7] ("DIY home surveillance with Webcam"), and Ex. 1033[8] ("Get Email Alerts when Alarm Sounds").

19. Prior to the filing date of Alarm.com '694 patent, the differences between: (1) web applications [that reside on a remote server and are delivered to a mobile device and run in the mobile device's web browser], and (2) client mobile applications or "native applications" [that are included on a mobile device] were known. *See* Ex. 2036[9] ("Native Mobile Apps v. Mobile Web Apps"); Ex. 2045 ("Encyclopedia Definition of: Native Mobile App"); Ex. 2046 ("Techopedia Definition of: Mobile App"); Ex. 2047 ("Techopedia Definition of: Native Mobile App"); Ex. 2064 ("HTML5 v. Native"); and Ex. 2065[10] ("Web Development for the iPhone").

20. In general, "native mobile applications" are more complex and inherit several pitfalls, including: (1) difficulties of distribution, (2) lack of a viral mechanism to spread apps as well as (3) resistance of most people to install applications. Ex. 2037[11] ("Sounding the Death Knell for Native Mobile Apps").

---

[7] The article "DIY home surveillance with Webcam" was posted on August 3, 2009 at http://www.alarmsystemreviews.com/unbiasednextalarm-customer-reviews.html (Exhibit 1032).

[8] The article "Get Email Alerts when Alarm Sounds" was posted on February 23, 2009 at http://homecontrolsblog.wordpress.com/2009/02/23/web-based-monitoring-andalarm-notification/) (Exhibit 1033).

[9] The article "Native Mobile Apps v. Mobile Web Apps" was posted on February 25, 2008 and, as such, qualifies as "prior art" against Alarm.com's application filed on May 18, 2010 (Ex. 2036).

[10] The article "Web Development for the iPhone" by Rich Warren was published on June 2008 and, as such, qualifies as "prior art" against Alarm.com's application filed on May 18, 2010 (Ex. 2065).

[11] The article "Sounding The Death Knell For Native Mobile Apps" by Carlo Longinoon was published on February 25, 2008 and, as such, qualifies as "prior art" against Alarm.com's application filed on May 18, 2010 (Ex. 2037).

As a result, many software developers were pushed toward mobile "web applications" instead of "native applications" because these mobile "web applications" are easier to distribute, faster to release from remote servers, have higher leverage on improving the base platform, and lower barrier to entry. *Id*., *see also* Ex. 2036 ("Native Mobile Apps v. Mobile Web Apps").

21. As described in connection with FF 1–16, iControl '365 application (which has been accorded the March 16, 2005 benefit date) provides a web-based solution to an integrated security system, shown in Figs. 1–2, where multiple applications (*e.g.*, End-User Application Components and user interface subsystems) are delivered from remote security system (iConnect) servers 104 to a mobile device 206, via a network 108, to allow an end user client at a mobile device 206 to remotely stay connected to a premise (home or office) and to remotely access, monitor, manage, and control operation of the security system 110, via the network 108. Ex. 1042.

22. iControl's "applications" that are delivered from remote security system (iConnect) servers 104 to a mobile device 206, via a network 108, for monitoring operations are known as "web-based applications" or "web applications."

23. iControl '365 application further suggests that these applications can also be custom-built for mobile devices. *Id.* at 13:12–16. In particular, iControl Claim 63 recites: "at least one application is custom-built for the mobile device." *Id.* Claim 62.

24. In early 2007, however, the first generation of iPhones released by Apple Inc. became available to the public that run on Apple's iOS mobile operating system. The Apple Store then opened in the summer of 2008 which allows: (1) users to browse and download applications that are developed with

Apple's iOS software developing kit (SDK), and (2) software developers to develop the so-called "native applications" specifically for Apple iOS platform. *See* Ex. 1012[12] ("Kleiner's Pick for the Killer iPhone App"); and Ex. 1013[13] ("Apple's Latest Opens a Developers' Playground").

25. The success of Apple iPhones and the Apple Store were unprecedented and the competition soared from other smartphone manufactures, such as Samsung Electronics, LG, HTC, Sony and Motorola running on Android operating system (OS) based on the Linux kernel developed by Google. *See* Ex. 1049 ("Apple Has Sold 450,000 iPads, 50 Million iPhones To Date"); Ex. 1050 ("iPhone Overtaken by Android in the US"). Because of the success of Apple iPhones and the Apple Store, hundreds of thousands of "native applications" for all types of applications have been developed by software developers for Apple iOS platform as well as other mobile device platforms such as Blackberry, Google Android, and Windows Mobile. Ex. 1050.

26. One example of the trend of software developers to develop "native applications" for Apple iOS platform and other mobile device platforms is demonstrated by iControl's "native mobile device monitoring applications" developed by iControl as evidenced in iControl's "App User Guide for iPhone," version 3.2, as part of the iControl system software released on December 16, 2008. *See* Ex. 1010,[14] p. 2 ("Overview of the Application" which describes:

---

[12] The article "Kleiner's Pick for the Killer iPhone App" by Peter Burrows was published on May 27, 2008 and, as such, qualifies as "prior art" against Alarm.com's application filed on May 18, 2010 (Ex. 1012).

[13] The article "Apple's Latest Opens a Developers' Playground" by John Markoff and Laura M. Holson was published on July 10, 2008 and, as such, qualifies as "prior art" against Alarm.com's application filed on May 18, 2010 (Ex.1013).

[14] iControl "Application User Guide for iPhone" was publicly available on December 16, 2008 (Ex.1010), and was provided to Alarm.com during litigation

"[T]he application allows you to access a core set of remote home monitoring and alarm system functions using your iPhone" and "[E]ach time you sign in to the app, your iPhone synchronizes with your site, downloads any pictures or video clips that were captured since you last signed in, provides you with any alarm updates, and updates all sensor and other device histories.").

2.

Alarm.com's Involved Patent (the '694 Patent)

27. Alarm.com '694 patent (filing date of May 18, 2010) discloses a monitoring system, shown in Fig. 1, that enables an end user client at a mobile device using such a "native mobile device monitoring application" loaded thereon to remotely access, monitor, and control operation of a home security system, via a network. Ex. 1001, Ex. 2001, Abstract, Fig. 1.

28. Alarm.com's Fig. 1 is reproduced below with additional markings for illustration.

---

between the parties before the U.S. District Court for the Eastern District of Virginia. However, Alarm.com argues that iControl's "App User Guide" is not prior art because: (1) iControl offers no evidence showing the content of the user guide was actually provided to customer or made publicly available in a manner that meets the criteria of 35 U.S.C. § 102, and (2) Alarm.com inventors had conceived the invention of Alarm.com '694 patent prior to December 16, 2008 and diligently reduced the invention to practice. *See* iControl Motion 1 (Paper 27) for unpatentability of Alarm.com's involved claims based on prior art. While iControl Motion 1 (Paper 27) need not be addressed, we will address the question of whether iControl's "App User Guide" constitutes as prior art for purposes of a no interference-in-fact analysis herein.

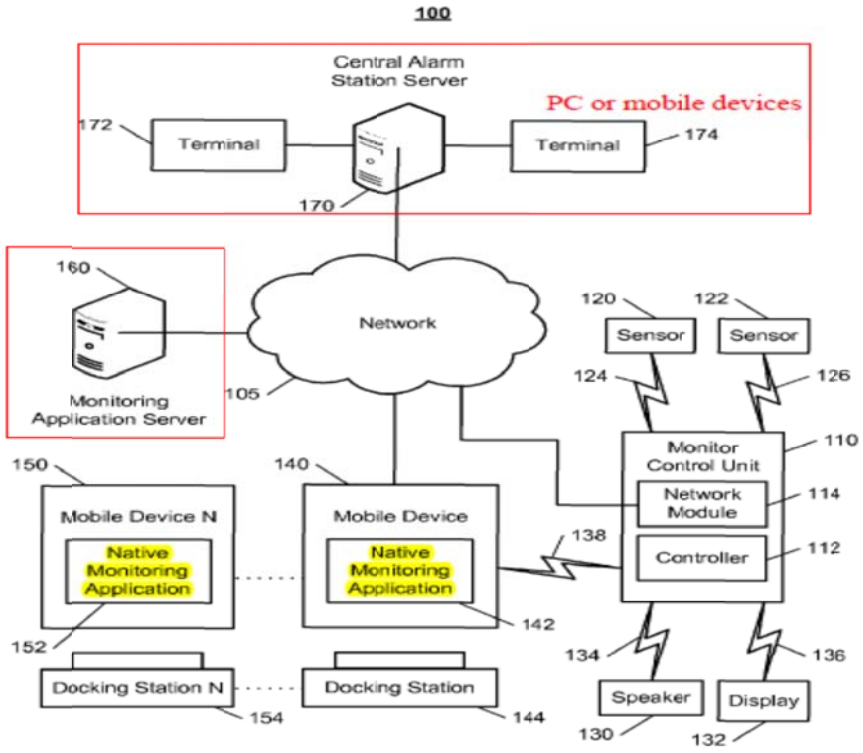


Fig. 1 shows a monitoring system 100 designed to permit an end user client to remotely access, monitor and control operation of a home security system using the mobile device 140 with a "native mobile device monitoring application" 142.

As shown in Alarm.com's Fig. 1, the monitoring system 100 includes: (1) a monitor control unit 110 with associated devices such as sensors 120, speaker 130 and display 132; (2) one or more mobile devices 140 each including a "native monitoring application"; and (3) remote security system servers in the form of a monitoring application server 160 and a central alarm station server 170 coupled to the monitor control unit 110 and associated devices, via a network 105, to provide monitoring services. *Id.* at 2:11–20, 4:44–64, 5:5–19, and Fig. 1.

29. For purposes of this interference and according to Alarm.com, a mobile device is described as:

> "The one or more mobile devices **140, 150** are devices that host and display user interfaces and that host one or more native applications (e.g., the native monitoring application **142, 152).** The one or more

> mobile devices **140, 150** may be cellular phones or non-cellular locally networked devices with displays. The one or more mobile devices **140, 150** may include *a cell phone, a smart phone, a tablet PC, a personal digital assistant ("PDA"), or any other portable device configured to communicate over a network and display information*. For example, implementations may also include Blackberry-type devices (e.g., as provided by Research in Motion), electronic organizers, iPhone-type devices (e.g., as provided by Apple), iPod devices (e.g., as provided by Apple) or other portable music players, other communication devices, and handheld or portable electronic devices for gaming, communications, and/or data organization."

Id. at 5:47–63 (emphasis added).

30. For purposes of this interference, a "native mobile device monitoring application" or "native monitoring application" is described as:

> "The native monitoring application **142, 152** refers to a *software/firmware program running on the corresponding mobile device that enables the user interface and features describe[d] below*. The one or more mobile devices **140, 150** may load or install the native monitoring application **142, 152** based on data received over a network or data received from local media. *The native monitoring application **142, 152** runs on mobile devices platforms, such as iPhone, iPod touch, Blackberry, Google Android, Windows Mobile, etc.*"

Id. at 6:48–58 (emphases added).

31. The "native monitoring application" 142, 152, shown in Alarm.com's Fig. 1, may be used, for example: (1) to check real time status of system and sensors, (2) to provide alerts based on monitoring system data, (3) to arm/disarm system, (4) to view live video on the mobile device, and (5) to leverage other features of the one or more mobile devices in providing monitoring services. *Id*. at 7:8–44.

32. According to Alarm.com:

> "The system **100** [not just a "native monitoring application"] *performs a synchronization process to synchronize a native mobile device monitoring application with a monitoring system for a property* **(210).** For instance, after the native mobile device monitoring application is loaded (e. g., downloaded) to a mobile device, the system **100** synchronizes the native mobile device monitoring application with a monitoring system for a property. The synchronization allows the native mobile device monitoring application to receive events detected by sensors in the appropriate monitoring system and send control commands to control operations related to the appropriate monitoring system."

Id. at 9:57–10:2 (emphasis added).

33. In order to perform "synchronization," Alarm.com describes two possible example implementations: First, the "native mobile device monitoring application" communicates directly with one or more local monitoring system components at the property. Second, the "native mobile device monitoring application" communicates with a remote monitoring application server 160 over a network 105. *Id*. at 10:17–19, 48–50.

34. In the first example implementation where the "native mobile device monitoring application" communicates directly with one or more local monitoring system components at the property:

> "[T]he system **100** may synchronize … The *synchronization may include a registration or pairing process, which enables the mobile device operating the native mobile device monitoring application to exchange data communications descriptive of sensor events detected by the monitoring system at the property* directly with the one or more local components of the monitoring system located at the property over the short range wireless communication protocol. For instance, the mobile device operating the native mobile device monitoring application may receive sensor data directly from sensors located at the property or may receive sensor data directly from a control panel that is located at the property and that receives sensor data directly from sensors located at the property."

Id. at 10:20–35 (emphasis added).

35. In the second (alternative) implementation where the "native mobile device monitoring application" communicates with a remote monitoring application server 160 over a network 105:

> "the synchronization process may involve the native mobile device monitoring application coordinating with the monitoring application server to synchronize with the monitoring system. For instance, *the native mobile device monitoring application may send authentication information (e.g., inputted username and password) to the monitoring application server to authenticate the native mobile device monitoring application to the monitoring application server. Once authenticated, the monitoring application server may handle the synchronization process*, which enables the native mobile device monitoring application to receive sensor event data detected by the monitoring system and send control commands to cause control of the monitoring system."

Id. at 10:50–63 (emphasis added).

B. ANALYSIS

1.

Alarm.com has the burden of proving that Alarm.com's claims and Claims 62–79 of iControl '365 application do not interfere.

> "An interference exists if the subject matter of a claim of one party would, if prior art, have anticipated or rendered obvious the subject matter of a claim of the opposing party and vice versa."

37 C.F.R. § 41.203(a).

This is the so-called "two-way" test for interference-in-fact. In order to establish no interference-in-fact, Alarm.com must establish that the "two-way" test is not met. In other words, Alarm.com can have this interference terminated on a judgment of no interference-in-fact if it can demonstrate, by motion, either party's claims would neither have anticipated, nor have rendered obvious, the subject

matter of the other party's claim or vice versa. *Yorkey v. Diab*, 605 F. 3d 1297, 1300 (Fed. Cir. 2010); *Winter v. Fujita*, 53 USPQ2d 1234 (BPAI 1999) (expanded panel).

The "two-way" test also incorporates the obviousness standard of 35 U.S.C. §103. 37 C.F.R. § 41.203(a). In deciding whether one party's claims are non-obvious in light of the opponent's claims, all the considerations necessary in reaching a conclusion of obviousness come into play. These include the underlying factual inquiries of: (1) the scope and content of the prior art; (2) the level of ordinary skill in the art; (3) the differences between the claimed invention and the prior art; and (4) any objective evidence of nonobviousness. *Graham v. John Deere Co.*, 383 U.S. 1, 17-18 (1966).

The obviousness determination must be made from the perspective of a hypothetical person of ordinary skill in the art who is presumed to have knowledge of all of the pertinent prior art. *See e.g., Custom Accessories, Inc. v. Jeffrey-Allan Indust., Inc.*, 807 F.2d 955, 963 (Fed. Cir. 1986); *Kimberly Clarke v. Johnson & Johnson*, 745 F.2d 1437, 1453 (Fed. Cir. 1984). Therefore, a movant attempting to show no interference-in-fact must provide an adequate evidentiary basis for evaluating the non-obviousness of the invention in light of: (1) the claim differences, (2) the scope and content of the prior art, (3) the level of ordinary skill in the art and (4) any evidence of secondary considerations. Meeting this burden typically involves proving a negative – that certain subject matter would not have been obvious to the person having ordinary skill in the art. As a negative burden, the threshold of proof is low, but there still is an evidentiary threshold that must be met. *See Cerveceria Centroamericana S.A. v. Cerveceria India, Inc.*, 892 F.2d 1021, 1024 (Fed. Cir. 1989).

A party attempting to show that the inventions are non-obvious, must show that there are differences from the opponent's invention. Differences alone, however, do not prove non-obviousness. It must be established that these differences are such that the invention as a whole would not have been obvious to a person having ordinary skill in the art. When secondary considerations are not relied upon, the movant must provide some evidentiary basis for holding that the differences render the invention non-obvious when the other is taken as a "primary reference." Thus, the movant must provide some evidence as to the level of ordinary skill in the art. Because the person of ordinary skill is assumed to know all the relevant prior art, the proffered evidence must provide a basis for concluding that the universe of relevant prior art would not provide a basis or reason for modifying the "primary reference" to account for the differences.

A movant might meet this negative burden by providing testimony from a person actually skilled in the particular art that he or she is unaware of any basis or reason to modify the subject matter of the "primary reference" to account for the differences as set forth by our Standing Order (Paper 2). Specifically, the Standing Order states:

> "A party may be able to satisfy its burden of production with testimony from a knowledgeable witness certifying that [1] there is no known prior art that would have overcome the differences between the subject matter of the count and the subject matter of the claim and that [2] the differences were not merely routine or conventional in the art."

Paper 2, SO ¶ 208.1.

Thus, the declarant might testify that the differences are (1) not conventional elements or other matters well known in the art and (2) that he or she is not aware of any prior art that would provide a reason or basis for modifying the "primary

reference." Where the evidence is sufficient, the movant will have established a prima facie case of non-obviousness.

2.

In this interference, the record shows that Alarm.com does not intend to put on a priority case. Alarm.com has elected to base its no interference-in-fact case maintaining *only* that the subject matter of iControl's claims would not have anticipated or rendered obvious the subject matter of Alarm.com's claims. Accordingly, Alarm.com has waived any argument based on the subject matter of Alarm.com's claims would not have anticipated or rendered obvious the subject matter of iControl's claims.

3.

iControl Application User Guide for iPhone (Exhibit 1010) as Prior Art

According to iControl, the iControl's "App User Guide for iPhone" (Ex. 1010), provides evidence of iControl's efforts to develop its own "native mobile device monitoring application" for iPhones, as part of the iControl system software released on December 16, 2008 which would render Alarm.com's claims obvious over iControl's claims in view of such art. iControl Opposition 1 (Paper 144) 14:26–15:1 (citing Ex. 1043 ¶ 159).

In its Reply (Paper 174), Alarm.com argues iControl's "App User Guide for iPhone" (Ex. 1010) does not qualify as prior art against Alarm.com's claims citing reasons presented in Alarm.com Opposition 1 (Paper 142) to iControl Motion 1 (Paper 27) for unpatentability of Alarm.com's involved claims based on prior art. As previously discussed, we need not address iControl Motion 1 (Paper 27).

However, to the extent that the prior art status of a reference under the provisions of 35 U.S.C. § 102 is relevant to reliance on a reference for the purposes of interference-in-fact and to the extent that Alarm.com's filing date is the relevant date by which to determine prior art status, iControl's "App User Guide" version 3.2 (Ex. 1010) was publically available more than a year before the application that became the involved Alarm.com patent was filed on May 18, 2010. Thus, we are not persuaded by Alarm.com's arguments that iControl improperly relied on Ex. 1010.

Specifically, iControl's "App User Guide" version 3.2 (Ex. 1010) bears a copyright notice of 2008 (Copyright@2008). Furthermore, Paul J. Dawes, who is the Chief Executive Officer (CEO) of iControl, testified that the iControl's "App User Guide for iPhone," version 3.2 (Ex. 1010) was formally released on December 16, 2008 to numerous customers that included in the release documents iControl's "App User Guide" for iPhone, Release 3.2, and that the customers to whom Release 3.2 was provided included: (1) Cincinnati Bell Inc. ("CBT") for use with its Honeywell security systems, (2) Comcast Corporation ("Comcast") for use with is General Electric SimonXT ("GE SimonXT") security system, (3) the ADT Corporation for use with its security and home automation services, and (4) Rogers Communications Inc. for use with its security and home automation services. *See* First Declaration of Paul Dawes (Ex. 1011, ¶¶ 5–11).

The formal release of iControl's "App User Guide" (Ex. 1010) on December 16, 2008 was memorized in an email dated on the same date, December 16, 2008 to employees re: iControl's customers (Ex. 1011), as reproduced below with additional markings for illustration:

Sent: Tuesday, December 16, 2008 2:28 PM
To: employees
Subject: FW: system version 3.2 release
Hi All,
I am pleased to announce the formal release of our 3.2 System today. Thanks to the whole team for all the hard work in delivering both our Honeywell and GE SimonXT configurations on-time (ok, one day late)! CBT and Comcast (lab trial) are updating to this release this week, with other customers to follow early next year.
You can see by the sheer number of components below that this has been quite an accomplishment by the whole company. The released versions are:
Server: 3.2.0-14
ServerAPI: 3.2.0-14
Relay: 3.2.0-14
AdminApp: 3.2.0-14
AdminHelp: 3.1.3-1
iHub 3.2.1-43
Main Portal: 3.2.0-14
Mobile: 3.2.0-5
Activation: 3.2.0-3
WebHelp: 3.2-4
MobileHelp: 3.2-4
iPhone: 3.2.0-31
TouchScreen: 3.2.0-29 (pending final approval)
Great Job all.
Thanks, Marc

Ex. 1011 confirms the formal release of iControl's "App User Guide," version 3.2 (Ex. 1010) on December 16, 2008 including the delivery of Honeywell and GE SimonXT configurations to CBT and Comcast on December 16, 2008.

Mr. Dawes' testimony (Ex. 1011, ¶ 5) is further corroborated by congratulatory emails sent by Marc Baum and Kevin Kraemer, respectively, touting "formal release" of Release to iControl customers in an email thread (Ex. 1021) as reproduced below with additional markings for illustration:

DOCUMENT NO. 46

From: Kevin Kraemer
Sent: Wednesday, December 17, 2008 1:55 AM
To: employees; Cheryl Jasper
Subject: RE: system version 3.2 release
Attachments: iPhone_App_User_Guide_(13004.12-002)_121508.pdf

I'd like to add my congratulations on a job well done. This is an important release for many of our partners – thank you all for your hard work in getting it out on time! Please take a moment to read through your long list of accomplishments below.
Note that all release-related documents, as well as other release details are on Twiki at:
http://twiki.icontrol.com/twiki/bin/view/Main/Release320Info
This release included the following customer-facing features:

Ex. 1021 confirms the release and availability of iControl's "App User Guide," version 3.2 (Ex. 1010) on December 16, 2008, via iControl online address at Twiki.

Alarm.com contends iControl's "App User Guide" is not prior art because iControl is alleged to offer no evidence showing the content of the user guide was actually provided to customers or made publicly available on December 16, 2008 in a manner that meets the criteria of 35 U.S.C. § 102. Paper 142, pp. 6–8. In particular, Alarm.com argues: (1) 35 U.S.C. § 102 does not contemplate "release" as grounds to establish a document as prior art; (2) the testimony of Paul J. Dawes (Ex. 1011) does not indicate that iControl's "App User Guide" was actually provided to numerous customers; and (3) the email thread (Ex. 1021) notes that "CBT and Comcast (lab trial) are updating this release this week, with other customers to follow early next year" and, as such, only corroborates the content of the release will be provided to CBT and Comcast and other customers at a future date. Paper 142, pp. 6–8.

iControl responds the First Declaration of Paul J. Dawes (Exhibit 1011) establishes that "On December 16, 2008, iControl formally released version 3.2 of the iControl system software ('Release 3.2') to numerous customers" (*Id.,* ¶5), that included in the release documents was the "iControl 'Application User Guide For iPhone, Release 3.2'" (*Id.,* ¶ 7), and that the customers to whom Release 3.2 was provided (or delivered) included Cincinnati Bell Inc. ("CBT"), Comcast Corporation ("Comcast"), The ADT Corporation, and Rogers Communications (*Id.,* ¶¶ 8-11). According to iControl, these customers, their employees and other customers are all clearly members of the interested public and the formal release is sufficient to qualify iControl's "App User Guide" as prior art. The statement in Ex. 1011 and Ex. 1021 that "CBT and Comcast (trial lab) are updating to this release this week, with other customers to follow early next year" involves actions undertaken by the customers (e.g., CBT and Comcast) after the release had been provided to them. Paper 173, 5:1–22 (citing Ex. 1011 ¶¶ 5–11).

We agree with iControl. "Public accessibility" is the touchstone in determining whether iControl's "App User Guide" constitutes a "printed publication" under 35 U.S.C. § 102. *In re Hall*, 781 F.2d 897, 898–899 (Fed. Cir. 1986). Our reviewing court has explained that a reference is "'publicly accessible'" upon a satisfactory showing that:

> (1) the "'document has been disseminated'"; or
>
> (2) "'otherwise made available to the extent that persons interested and ordinarily skilled in the subject matter or art exercising reasonable diligence, can locate it and recognize and comprehend therefrom the essentials of the claimed invention without need of further research or experimentation.'"

Bruckelmyer v. Ground Heaters, Inc., 445 F.3d 1374, 1378 (Fed. Cir. 2006) (quoting *In re Wyer*, 655 F.2d 221, 226 (CCPA 1981)).

Contrary to Alarm.com's arguments, the evidence shows that iControl's "App User Guide," version 3.2 (Ex. 1010) was expressly identified, provided and delivered, or otherwise "disseminated" to persons interested in the subject matter, *i.e.*, iControl's customers including Cincinnati Bell Inc. ("CBT"), Comcast Corporation ("Comcast"), ADT Corporation, and Rogers Communications. *See* Ex. 1011, ¶¶ 5–11), and Ex. 1021. As such, we find iControl's "App User Guide," version 3.2 (Ex. 1010) constitutes a prior art "printed publication" bar under 35 U.S.C. § 102(b) and, as such, cannot be antedated by Rule 131 Declarations[15] of Alison Slavin (Ex. 2063) and Brandron O'Rourke (Ex. 2062).

[15] We note that Alarm.com '694 patent has a filing date of May 18, 2010. Alarm.com '649 patent was not accorded the benefit of Provisional App 61/179,215 ("the provisional"), and Alarm.com did not file a motion to accord the benefit, despite the Board's authorization. Paper 19. As such, the effective filing date of Alarm.com '694 patent is May 18, 2010. In contrast, iControl's "App User Guide" version 3.2 (Ex. 1010) is found to be publicly available on December 16,

4.

Claim Construction

In determining patentability over the prior art, the name of the game is the claim. *In re Hiniker Co.*, 150 F.3d 1362, 1369 (Fed. Cir. 1998). Claim terms of an involved patent in an interference are given their broadest reasonable construction as they would be understood by one of skill in the art in light of the specification. *Rolls-Royce PLC v. United Technologies Corp.*, 603 F.3d 1325, 1330 (Fed. Cir. 2010). "There are only two exceptions to this general rule: 1) when a patentee sets out a definition and acts as his own lexicographer or 2) when the patentee disavows the full scope of a claim term either in the specification or during prosecution." *Thorner v. Sony Computer Entm't Am. LLC*, 669 F.3d 1362, 1365 (Fed. Cir. 2012).

We look to Alarm.com's disclosure and file history to see if they provide a definition for disputed claim terms. Otherwise, we give them their "ordinary and customary meaning" in the light of the specification that "the term would have to a person of ordinary skill in the art in question at the time of the invention, i.e., as of the effective filing date of the patent application." *Phillips v. AWH Corp.*, 415 F.3d at 1313 (Fed. Cir. 2005) (en banc).

2008 – more than a year relative to Alarm.com's effective filing date of May 18, 2010. We recognize our finding that iControl's "App User Guide," version 3.2 (Ex. 1010) constitutes a prior art "printed publication" bar under 35 U.S.C. § 102(b) appears at odds with the position advanced by iControl's Motion 1 (Paper 27) that iControl's "App User Guide," version 3.2 (Ex. 1010) is a § 102(a) prior art and, as such, can be antedated by Rule 131 Declarations as submitted by Alarm.com Opposition 1 (Paper 142). Nevertheless, iControl's "App User Guide" version 3.2 (Ex. 1010) is a prior art "printed publication" bar under 35 U.S.C. § 102(b) and, as such, cannot be antedated by Rule 131 Declarations of Alison Slavin (Ex. 2063) and Brandron O'Rourke (Ex. 2062).

In the present interference, analysis of no interference-in-fact depends on the meaning of several claim terms from independent claims 1, 21, and 41 of Alarm.com '694 patent that correspond to the Count. Paper 1 at p. 4. The disputed claim terms are: (1) "a mobile device", (2) "a native mobile device monitoring application", and (3) "a synchronization process" as recited in Claims 1, 21, and 41 of Alarm.com '694 patent corresponding to the Count. As per *Agilent*, these disputed terms are to be construed in light of the host disclosure, *i.e.*, Alarm.com's disclosure and file history, which we will address each claim term identified by Alarm.com in turn.

1. "Mobile Device"

Alarm.com, relying on Dr. Malek's testimony (Ex. 2004, ¶¶ 29–32 and 34) proffers a broad construction of the claim term "mobile device" to simply mean a small, handheld computing device. Paper 66, p. 6.

iControl responds such proffered construction is nowhere defined in either Alarm.com '694 patent or iControl '365 application. According to iControl, Alarm.com '694 patent describes that "mobile devices 140, 150 may include a cell phone, a smart phone, a tablet PC, a personal digital assistant (PDA), or any other portable device configured to communicate over a network and display information." Ex. 1001, 5:51–57; FF 29. Based on that description, iControl contends the term "mobile device" in the claims of Alarm.com '694 patent should be construed narrowly as "any portable electronic device configured to communicate over a network and display information." iControl Opposition 1, Paper 144, p. 3.

Upon reviewing the host disclosure, *i.e.*, Alarm.com's disclosure and file history, we find iControl's proffered claim construction of the term "mobile device" is consistent with the specification of Alarm.com '694 patent. Ex. 1001,

5:51–57; FF 29. As such, we adopt iControl's claim construction that "mobile device" is defined to mean "any portable electronic device configured to communicate over a network and display information."

2. "Native Mobile Device Monitoring Application"

Relying on Dr. Malek's testimony (Ex. 2004, ¶¶ 29–32 and 35), Alarm.com also proffers a construction of the claim term "native mobile device monitoring application" to mean a "software/firmware monitoring program in executable form that is written for a specific mobile device platform, such as iPhone, iPod touch, Blackberry, Google Android or Windows Mobile." Paper 66, p. 6.

iControl responds such proffered construction is improper because: (1) Dr. Malek's testimony is without support or conclusory, and (2) nowhere does Alarm.com '694 patent require that the "native mobile device monitoring application" must be "in executable form" or that "written for a specific mobile device platform, such as iPhone, iPod Touch, Blackberry, Google Android or Windows Mobile." iControl Opposition 1, Paper 144, pp. 4–5. According to iControl, Alarm.com '694 patent only teaches that the "native monitoring application" refers to "a software/firmware program running on the corresponding mobile device that enables the user interface and features" and also runs on various mobile devices platforms, such as iPhone, iPod touch, Blackberry, Google Android or Windows Mobile. *Id*. at 5 (citing Ex. 1001, 6:49–58); FF 30. Based on that description, iControl relies on its own expert, Mr. Tipton Cole (Ex. 1043, ¶¶ 120–123) to construe the term "native mobile device monitoring application" more broadly as: "a program running on a mobile device that enables use of the mobile device as a user interface and controller for the monitoring system." Paper 144, pp. 4–5.

Upon reviewing Alarm.com's disclosure, we find neither party's claim construction of the term "native monitoring application" is consistent with the specification of Alarm.com '694 patent. On one hand, Alarm.com's proffered construction does not account for any firmware program, user interface or monitor functions. On the other hand, iControl's proffered construction is too broad and does not differentiate the distinctions between the so-called "web applications" as disclosed by iControl '365 application and "native applications" as disclosed by Alarm.com's '694 patent. We also understand that "a native mobile device monitoring application" is built or written specifically for a particular mobile device platform, such as iPhone, iPod Touch, Blackberry, Google Android or Windows Mobile, as Alarm.com argues. Paper 66, p. 6; *see also* Ex. 2036 ("Native Mobile Apps v. Mobile Web Apps"); Ex. 2045 ("Encyclopedia Definition of: Native Mobile App"); Ex. 2046 ("Techopedia Definition of: Mobile App"); Ex. 2047 ("Techopedia Definition of: Native Mobile App"); Ex. 2064 ("HTML5 v. Native"); and Ex. 2065 ("Web Development for the iPhone").

For example, if a native application is written for Apple iOS, that native application can only run on Apple products, such as an iPhone, and does not run on Android devices. If a native application is intended to run on both Apple iOS and Android devices, then two different versions of the native application must be created separately for Apple iOS and Android devices. *See* Ex. 2064 ("HTML5 v. Native").

Based on our review of Alarm.com's disclosure (FF 21–29) and the state of the art (FF 16–26), we accept part of the parties' proffered claim constructions and construe the term "native mobile device monitoring application" to mean "a software/firmware program in executable form that is written for a specific mobile device platform, such as iPhone, iPod Touch, Blackberry, Google Android or

Windows Mobile, and enables use of the mobile device as a user interface and controller for the monitoring system."

3. "Synchronization Process"

Alarm.com initially does not proffer a construction of the term "synchronization process to synchronize the native mobile device monitoring application with the monitoring system." Paper 66, p. 6. Instead, Alarm.com contends that Alarm.com's "synchronization process **to synchronize** the native mobile device monitoring application with the monitoring system" is *not* the same as iControl's "synchronization **to associate** the mobile device with the monitoring system." *Id*. at 6 (citing Ex. 2004, ¶ 36) (emphasis in original).

Relying on Mr. Tipton's testimony (Ex. 1043, ¶¶ 43–44, 48), iControl proffers a construction of that term to mean "performing a registration or authentication process that allows the NMDMA [native mobile device monitoring application] to receive events from and sends commands to the monitoring system." iControl Opposition 1, Paper 144, p. 6 (citing Ex. 1043, ¶ 44). According to iControl, that construction is consistent with Alarm.com's disclosure.

For example, the Alarm.com '694 patent describes two possible example implementations of a "synchronization process." In particular, Alarm.com '694 patent describes: "The system 100 performs a synchronization process to synchronize a native mobile device monitoring application with a monitoring system for a property (210)… The synchronization allows the native mobile device monitoring application to receive events detected by sensors in the appropriate monitoring system and send control commands to control operations related to the appropriate monitoring system." Ex. 1001, 9:59–10:2; FF 32–35. "The synchronization may include a registration or pairing process" for the case in which "the native mobile device monitoring application communicates directly

with one or more local monitoring system components at the property." Ex. 1001, 10:17–23; FF 34. Alternatively, for synchronization involving a remote server, the synchronization process may involve the native mobile device monitoring application sending "authentication information (*e.g.*, inputted username and password) to the monitoring application server to authenticate the native mobile device monitoring application to the monitoring application server." Ex. 1001, 10:48–63; Claim 3; FF 35.

In its Reply (Paper 174) and relying on Dr. Malek's testimony (Ex. 2052), Alarm.com argues iControl's construction is overly broad and inconsistent with the ordinary meaning of the term "synchronization" as used in Alarm.com's '694 patent. Paper 174, p. 2 (citing Ex. 2052 ¶¶ 23–24). According to Alarm.com, the '694 patent describes a "synchronization process" after an authentication process and that "synchronization process" is something more than just "a registration or an authentication process," as iControl asserts. *Id*. at 2 (citing Ex. 2052, ¶ 23; Ex. 2001, 10:48–11:15).

Alarm.com further argues the ability "to receive events from and send commands to the monitoring system" represents only an ability to communicate and does not represent synchronization. *Id*. According to Alarm.com, the ordinary meaning of the term "synchronization" refers to consistency in state and time between items that are synchronized. *Id*. at 3.

During the oral hearing conducted on February 26, 2015, Alarm.com counsel reiterated the ordinary meaning of the term "synchronization" as follows:

> "So Alarm.com's position has been that *synchronization requires some sort of consistency in state and time*. If you think about synchronized swimming for swimmers to be synchronized, they have to be synchronized in state. Their movements have to be the same. They also have to be synchronized in time. Those movements have to occur at the same time for synchronization to occur."

Transcript (Paper 198) 10:19–25 (emphasis added).

When asked how Alarm.com would have the Board construe the claim term "synchronization," Alarm.com counsel responded:

> "I would construe it consistent with what we have advanced in the brief, that there has to be a consistency in state and time with the items that are synchronized. We have a synchronization between the mobile application. It is the application itself that is synchronized with the monitoring system.
>
> So that when you perform that synchronization process, you get a consistency in state and time between the two items synchronized, the mobile application and the monitoring system. And with that, that allows you, and based on that synchronization, you can then perform the other actions in the claim, but it is that first synchronization process that really has to be considered.
>
> And I think the ordinary meaning of synchronization and synchronization process would require that consistency in state and time."

Id. at 15:8–25.

We are not persuaded by Alarm.com's arguments and proffered evidence. We acknowledge the term "synchronization" may have an industry understood definition and that "ordinary" and "customary" meaning of "synchronization" may include "some sort of consistency in state and time" as Alarm.com advocates. Paper 174, p. 2–3. However, it is the use of the words in the context of the written description and customarily by those skilled in the relevant art that accurately reflects both the "ordinary" and the "customary" meaning of the terms in the claims. *Ferguson Beauregard/Logic Controls, Div. of Dover Res., Inc. v. Mega Sys., LLC*, 350 F.3d 1327, 1338 (Fed. Cir. 2003).

> "The claims, of course, do not stand alone. Rather, they are part of a 'fully integrated written instrument,' … consisting

> principally of a specification that concludes with the claims. For that reason, claims 'must be read in view of the specification' . . . . [T]he specification 'is always highly relevant to the claim construction analysis. Usually, it is dispositive; it is the single best guide to the meaning of a disputed term.'"

Phillips, 415 F.3d at 1315(citations omitted). In other words, Alarm.com's disclosure is the best guide to the meaning of the term "synchronization." The broadest reasonable meaning of disputed terms is "their ordinary usage *as they would be understood by one of ordinary skill in the art*, taking into account whatever enlightenment by way of *definitions* or otherwise that may be afforded by the *written description* contained in the applicant's specification." *In re Morris*, 127 F.3d 1048, 1054 (Fed. Cir. 1997) (emphasis added).

The Federal Circuit has also emphasized the use of intrinsic evidence, *i.e.*, the specification and prosecution history, as the primary source of identifying the "ordinary and customary meaning" of a claim term. *Phillips*, 415 F.3d at 1313–18. Only if ambiguities still exist, then extrinsic evidence, such as dictionary or Wikipedia definitions and technical references as well as expert witness testimony may be considered. The Federal Circuit has viewed "extrinsic evidence in general as less reliable than the patent and its prosecution history in determining how to read claim terms, for several reasons" including, for example, "there is a virtually unbounded universe of potential extrinsic evidence of some marginal relevance that could be brought to bear on any claim construction question." *Id.* at 1318.

In this interference, the claim term "synchronization" is not expressly defined in Alarm.com's disclosure. Neither "state" nor "time" is required or described in connection with the term "synchronization" in Alarm.com's disclosure. Nevertheless, Alarm.com '694 patent provides sufficient written description to guide us as to the meaning of the term "synchronization."

For example, Alarm.com '694 patent describes two possible example implementations of "synchronization." In the first implementation where the "native mobile device monitoring application" communicates directly with one or more local monitoring system components at the property:

> "[T]he system **100** may synchronize … The *synchronization may include a registration or pairing process, which enables the mobile device operating the native mobile device monitoring application to exchange data communications descriptive of sensor events detected by the monitoring system at the property* directly with the one or more local components of the monitoring system located at the property over the short range wireless communication protocol. For instance, the mobile device operating the native mobile device monitoring application may receive sensor data directly from sensors located at the property or may receive sensor data directly from a control panel that is located at the property and that receives sensor data directly from sensors located at the property."

Ex. 1001, 10:22–35 (emphasis added).

In the second (alternative) implementation where the "native mobile device monitoring application" communicates with a remote monitoring application server 160 over a network 105 (similar to iControl's Figs. 1–2):

> "the synchronization process may involve the native mobile device monitoring application coordinating with the monitoring application server to synchronize with the monitoring system. For instance, the native mobile device monitoring application may send authentication information (e.g., inputted username and password) to the monitoring application server to authenticate the native mobile device monitoring application to the monitoring application server. *Once authenticated, the monitoring application server may handle the synchronization process,* which enables the native mobile device monitoring application to receive sensor event data detected by the monitoring system and send control commands to cause control of the monitoring system."

Id. at 10:50–63 (emphasis added).

Based on Alarm.com's disclosure (FF 21–29), we adopt iControl's proffered construction of the term "synchronization" to mean "performing a registration or authentication process that allows the native mobile device monitoring application to receive events from and sends commands to the monitoring system" because iControl's proffered construction is more consistent with Alarm.com's disclosure. iControl Opposition 1, Paper 144, p. 6 (citing Ex. 1043, ¶ 44). For example, in both example implementations described by Alarm.com '694 patent, the term "synchronization" may include registration or authentication to enable a mobile device running a "native mobile device monitoring application" to exchange data with the monitoring system. Ex. 1001, 10:22–35, 50–63. As such, we find iControl's construction of the term "synchronization" sufficiently broad to encompass both example implementations disclosed by Alarm.com '694 patent.

5.

Legal Standard for 35 U.S.C. §§ 102(b) and 103(a)

Having determined the meaning of the claims, we turn to whether iControl's claims would have anticipated or rendered obvious Alarm.com's claims. To establish anticipation, a party must show that a prior art reference expressly or inherently describes each claim limitation arranged as in the claim said to be anticipated. *Finisar Corp. v. DirecTV Group, Inc.*, 523 F.3d 1323, 1334–35 (Fed. Cir. 2008); *Net MoneyIN, Inc. v. VeriSign, Inc.*, 545 F.3d 1359, 1371 (Fed. Cir. 2008). Whether a reference anticipates a claim is a question of fact. *In re Baxter Travenol Lab.*, 952 F.2d 388, 390 (Fed. Cir. 1991).

Obviousness is an issue of law resolved on the basis of underlying facts. *Graham v. John Deere Co.*, 383 U.S. 1, 17 (1966), reaffirmed in *KSR Int'l Co. v. Teleflex Corp.*, 550 U.S. 398, 406–7 (2007). The underlying facts includes: (1) the

scope and content of the prior art, (2) any differences between the claimed subject matter and the prior art, (3) the level of skill in the art, and (4) where in evidence, so-called secondary considerations. *Graham v. John Deere Co. of Kansas City*, 383 U.S. 1, 17-18 (1966). *See also KSR*, 550 U.S. at 406-07 ("While the sequence of these questions might be reordered in any particular case, the [*Graham*] factors continue to define the inquiry that controls.").

Alarm.com determines that a person of ordinary skill in the art is one with at least a bachelor degree in computer science or engineering (or, alternatively, at least 5 years of professional programming experience), plus (in both cases) at least one year's experience with developing applications for distributed systems. Paper 66, pp. 9–10; Ex. 2004, ¶ 25.

iControl responds that a person of ordinary skill in the art is one with at least a bachelor degree in computer science or electrical engineering and at least two years' experience with software applications in a network environment. Paper 144, pp. 9–10; Ex. 1043, ¶ 24. iControl's expert, J. Tipton Cole, testifies:

> "With that level of training and experience, one would be able to: 1) write software applications that communicate with the monitor control unit; 2) analyze the data received from the monitor control unit for presentation to the user; and 3) accept instructions from the user (or generate instructions in response to the incoming data) for the monitor control unit to set the appropriate states for the various devices that make up the monitoring system."

Ex. 1043, ¶ 24.

Neither party's assessed level of ordinary skill in the art is disputed. For purposes of this interference, we find the level of skill in the art in terms of degrees obtained is less helpful than defining it in terms of what such a person would have known and what the person would have been able to do. *Argyropoulos v. Swarup*,

56 USPQ2d 1795, 1807 (BPAI 2000). We believe that the prior art itself can also reflect what one skilled in art would have known. *In re GPAC, Inc.*, 57 F.3d 1573, 1577 (Fed. Cir. 1995) (level of skill in the art can be determined by reference to prior art of record).

6. *Anticipation under 35 U.S.C. § 102(b)*

Alarm.com contends none of iControl's claims anticipate any of Alarm.com's claims because iControl's claims do not recite:

> "*a native mobile device monitoring application* loaded onto a mobile device that is provided separately from the monitoring system by a company that is different than a company that provides the monitoring system, *the native mobile device monitoring application including instructions that, when executed by the mobile device, cause the mobile device to perform operations* comprising … performing a *synchronization process to synchronize* the native mobile device monitoring application with the monitoring system that is configured to monitor the property."

Paper 66, pp. 5–6; Ex. 2011, Claim 1 (emphasis added). In particular, Alarm.com acknowledges iControl's dependent claim 63 recites "at least one of the applications is custom-built for the mobile device" but argues that an application that is custom-built for the mobile device is not necessary "a native mobile device monitoring application." Paper 66, pp. 5–6; Paper 174, pp. 3–4 (citing Ex. 2065).

iControl responds that one skilled in the art would have believed that: (1) the custom-built application of iControl Claim 63 is Alarm.com's claimed "native mobile device monitoring application," and (2) the custom-built application of iControl Claim 63 synchronizes with the monitoring system. Paper 144, p. 8 (citing Ex. 1043, ¶ 143).

During the oral hearing conducted on February 26, 2015, when asked to explain the differences between a "native application" and a "custom-built application," counsel for Alarm.com responded:

> "A native application requires the application to be on the device. Custom-built just means that it is customized for a particular application. It doesn't give you any information on where that application resides or what that application is doing. It just means that it is custom, it is modified."

Transcript (Paper 198) 19:4–9.

We are persuaded by Alarm.com's arguments. As correctly noted by Alarm.com, custom-built applications can be customized for a particular function. Paper 174, pp. 3–4. We find Alarm.com's position is consistent with iControl '365 application which describes "custom-built" applications as "complex applications where integrated security system content is integrated into a broader set of application features." Ex. 1042, 13:12–16; FF 15. For example, web applications as described in iControl '365 application can be customized for specific mobile devices, but would not be "native" to those devices. Nevertheless, we note these "custom-built" applications can also include "native applications" if they are written specifically for a particular mobile device platform such as Apple iOS or Google Android. However, in the absence of such an express teaching, we find the "custom-built" applications as disclosed by iControl '365 application do not include "native applications" as those "native applications" have a specific meaning within the art, as outlined in our claim construction of that term.

Based on our claim construction of the term "synchronization" and the term "native mobile device monitor application" as discussed above, and the differences between: (1) "web applications" that reside on a remote server and are delivered to a mobile device and run on a mobile device's web browser, such as those disclosed

by iControl's disclosure, and (2) "native applications" that are included on a mobile device as disclosed by Alarm.com's disclosure, we are persuaded by Alarm.com's arguments and find Alarm.com's claims are not anticipated by iControl's claims.

7.

Obviousness under 35 U.S.C. § 103(a)

Alarm.com argues none of iControl's claims render obvious any of Alarm.com's claims because: (1) at the time of Alarm.com's disclosure, it was known to associate mobile devices with monitoring systems and use associated mobile devices to remotely interact with monitoring systems through web interfaces as disclosed, for example, by iControl's disclosure (FF 1–16), (2) "native mobile device applications" were being developed in other contexts at the time of Alarm.com's disclosure, and (3) yet those "native mobile device applications" were not used with monitoring systems, much less used in performing a synchronization process to synchronize the native mobile device monitoring application with the monitoring system that is configured to monitor the property in the manner recited in Alarm.com's claims. Paper 66, pp. 10–11.

As evidence of the non-obviousness of Alarm.com's claims in view of iControl's claims and the state of the art, Alarm.com submits: (1) a Declaration from the inventor of the '694 patent, Alison Slavin, to confirm that she is unaware of any prior art or other reasons that account for the differences between Alarm.com's claims and iControl's claims and the state of the art (Ex. 2004), (2) a Declaration from industry Expert, Dr. Malek, to confirm that he is unaware of any prior art or other reasons that would account for the differences between Alarm.com's claims and iControl's claims and the state of the art (Ex. 2004), and

(3) the prosecution history of U.S. Patent Application No. 13/735,193 (hereinafter "the '193 application"), a continuation application from the '694 patent, to confirm that the differences between Alarm.com's claims and iControl's claims and the state of the art are not obvious (Ex. 2008). *Id*. at 11–15.

We are not persuaded by Alarm.com's arguments and proffered evidence of non-obviousness. At the outset, we note Alarm.com may not limit its consideration of prior art within any nonobviousness analysis to only those pre-existing in the record of the involved cases, including: (1) U.S. Patent No. 6,400,265 issued to Saylor, which is owned by Alarm.com (Ex. 2069), (2) U.S. Publication No. 2009/0066488 issued to Qiahe, which was cited during prosecution of Alarm.com '694 patent (Ex. 2009), (3) U.S. Publication No. 2009/0062964 issued to Sullivan, which was also raised during prosecution of Alarm.com '694 patent (Ex. 2010), and (4) other examples of what Alarm.com characterizes as the state of the art, including: (i) HP OpenView (Ex. 2012 – Ex. 2017), (ii) LinuxMCE (Ex. 2021 – Ex. 2023), and (iii) European Patent No. 1 097 409 B1 (Ex. 2011). Paper 66, pp. 6–9. While it certainly is true that Alarm.com cannot be reasonably expected to account for the entire body of prior art in existence in the world including that which is unknown to Alarm.com, but it can be, and indeed is, expected to account for that prior art which its inventors are aware or is otherwise known to party Alarm.com, including those provided to the parties during litigation before the U.S. District Court for the Eastern District of Virginia, such as iControl's iPhone App User Guide for iPhones. Paper 144, 11:19–23 (citing Ex. 1010). *See Pechiney Emballage Flexible Europe v. Cryovac Inc.*, 73 USPQ2d 1571 (BPAI 2004). Alarm.com's focus upon only selected "prior art of record" reflects a misidentification of the nature of Alarm.com's motion, the status quo, and the burden of proof.

In this interference, Alarm.com must begin with the obviousness conclusion already presumed, and prove the negative — nonobviousness. The same underlying factual inquiries present under *Graham* are involved.

Alarm.com must show that those skilled in the art would not have found the two features of Alarm.com's claims: (1) "a native mobile device monitoring application" and (2) "a synchronization process to synchronize the native mobile device monitoring application with the monitoring system" obvious in view of iControl's claims. More importantly, Alarm.com must also demonstrate that the knowledge in the art at the time, when combined with iControl's claims, would have rendered Alarm.com's claimed subject matter obvious. Alarm.com might overcome its burden by showing, in light of the *Graham* factors, those in the art would not have developed the subject matter claimed using common sense and the knowledge available and motivated by needs and problems faced at the time. *See KSR Int'l v. Teleflex, Inc.*, 127 S.Ct. at 1741–42 (2007). Such a showing often comes in the form of witness testimony about what those in the art did or did not know. Alternatively, Alarm.com might show: (1) there were unexpected results, (2) the applicable art taught away from any modifications of the subject matter or (3) the knowledge in the art undermined the very reason being proffered as to why a person of ordinary skill would have combined the known elements. *See DePuy Spine, Inc. v. Medtronic Sofamor Danek, Inc.*, 567 F.3d 1314, 1326 (Fed. Cir. 2009). In any case, if a party presents opinion testimony from a witness, the testimony must be supported with factual evidence. *Cf. Upjohn Co. v. Mova Pharm. Corp*., 225 F.3d 1306, 1311 (Fed. Cir. 2000).

In this motion, Alarm.com has not carried its burden of proof, *viz.*, to show that Alarm.com's claims would not have been obvious in view of iControl's claims. Specifically, Alarm.com fails to properly account for the knowledge in the

art, including: (1) the trend in the software industry after the enormous success of Apple iPhone and the Apple Store to develop "native applications" for Apple iOS platform as well as other mobile device platforms such as Blackberry, Google Android, or Windows Mobile (Ex. 1012 and Ex. 1013), and (2) iControl's own efforts to develop iControl's own "native mobile device monitoring applications" in the form of iControl's "App User Guide for iPhones," version 3.2 (Ex. 1010) as a commercial alternative for an integrated security system disclosed by iControl '365 application (FF 25–26).

Dr. Malek's testimony (Ex. 2004, ¶¶ 40–68) is based only on selected prior art of record that he has analyzed and Alarm.com has not pointed us to any representation by Dr. Malek that he has analyzed all the prior art which its inventors are aware of, or is otherwise known to party Alarm.com, and what those in the art would or would not have done given the knowledge of iControl's claimed subject matter and any other relevant prior art. Alarm.com has made clear that its position is based at most only on the prior art of record, and not on the basis of all that which Alarm.com or its technical witness is aware. *See* iControl Opposition 1 (Paper 144) at 10:22–23. In addition, Dr. Malek's testimony fails to account for the differences between the subject matter of Alarm.com's claims and the subject matter of iControl's claims, which were not merely routine or conventional in the art, as required by SO ¶ 208.1.

With respect to the prosecution history of U.S. Patent Application No. 13/735,193, a continuation application from the '694 patent, which Alarm.com argues as evidence of non-obviousness because the Examiner found those differences to be non-obvious (Paper 66, pp. 13–15; Ex. 2001), we are not persuaded for several reasons. First, the Examiner's reasons for allowance (Ex. 2008) are not dispositive of there being no interference-in-fact. Second, as

correctly noted by iControl, the Examiner's reasons for allowance (Ex. 2008) were based solely on consideration of U.S. Publication No. 2009/0062964 issued to Sullivan, which was already raised during prosecution of Alarm.com '694 patent (Ex. 2010). Paper 144, pp. 12 (citing Ex. 2004, and Ex. 2006 – Ex. 2008). Third, the Examiner did not have the benefit of iControl's additional evidence and explanations of obviousness as presented in this interference. Fourth, the Examiner was later convinced that an interference was warranted. Paper 1, p. 1–6.

For the foregoing reasons, Alarm.com has not shown that it is entitled to the relief requested, *i.e.*, that there is no interference-in-fact.

Even assuming Alarm.com has met his burden of proof, we are not persuaded that the differences between the subject matter of Alarm.com's claims and the subject matter of iControl's claims (presumed to be prior art for the purpose of an interference-in-fact analysis) would have been nonobvious to those skilled in the art, including: (1) "a native mobile device monitoring application" and (2) "a synchronization process to synchronize the native mobile device monitoring application with the monitoring system."

Rather, we find these features of Alarm.com's claims would have been obvious in view of all claims of iControl '365 application (as prior art). Why? Because an artisan of ordinary skill is presumed to know all the relevant prior art at the time of Alarm.com's invention (during the 2007–2010 timeframe), including, for example:

(1) the differences between "web applications" [that reside on a remote server and are delivered to a mobile device and run in the mobile device's web browser] and "native applications" [that are included on a mobile device] (Ex. 2036 "Native Mobile Apps v. Mobile Web Apps"; 2065 "Web Development for iPhone"; and FF 19);

(2) the advantages and disadvantages of these "web applications" and "native applications (Ex. 2036 "Native Mobile Apps v. Mobile Web Apps"; Ex. 2037 "Sounding the Death Knell for Native Mobile Apps"; and FF 20);

(3) the enormous success of Apple iPhones, the Apple Store and competition from other smartphone manufactures, such as Samsung Electronics, LG, HTC, Sony and Motorola running on Android operating system (OS) based on Linux kernel developed by Google (Ex. 1049 "Apple has sold 450,000 iPads, 50 Million iPhones to date"; Ex. 1050 "iPhone overtaken by Android in the US"; and FF 24–25); and

(4) because of the enormous success of Apple iPhone and the Apple Store, the trend in the software industry (during the 2007–2010 timeframe) was such that all software developers clamored to develop "native applications" for Apple iOS platform as well as other mobile device platforms such as Blackberry, Google Android, or Windows Mobile, including, for example: iControl's own efforts to develop iControl's own "native mobile device monitoring applications" as a commercial alternative for iControl's integrated security system disclosed by iControl '365 application (Ex. 1010, and FF 25–26). *See* iControl Opposition 1 (Paper 144) at 14:8–15:7.

As expressly explained by iControl's "App User Guide" version 3.2 (Ex. 1010, p. 2 "Overview of the Application": "[T]he application allows you to access a core set of remote home monitoring and alarm system functions using your iPhone" and "[E]ach time you sign in to the app, your iPhone synchronizes with your site, downloads any pictures or video clips that were captured since you last signed in, provides you with any alarm updates, and updates all sensor and other device histories."). *See* iControl Opposition 1 (Paper 144) at 15:7–17. Thus, the

artisan is presumed to have the technical competence and sufficient skill to develop the disputed features of Alarm.com's claims.

Evidence of Nonobviousness Based on Secondary Considerations

Factual inquiries for an obviousness determination include secondary considerations based on evaluation and crediting of objective evidence of nonobviousness. *Graham*, 383 U.S. at 17. Notwithstanding what the teachings of the prior art would have suggested to one with ordinary skill in the art at the time of Alarm.com's invention, the totality of the evidence submitted, including objective evidence of nonobviousness, may lead to a conclusion that the challenged claims would not have been obvious to one with ordinary skill in the art. *In re Piasecki*, 745 F.2d 1468, 1471–72 (Fed. Cir. 1984). Secondary considerations may include any of the following: long-felt but unsolved needs, failure of others, unexpected results, commercial success, copying, licensing, and praise. *See Graham*, 383 U.S. at 17; *Leapfrog Enters.*, 485 F.3d at 1162.

Evidence of nonobviousness, however, must be commensurate in scope with the claimed invention. *In re Kao*, 639 F.3d 1057, 1068 (Fed. Cir. 2011) (citing *In re Tiffin*, 448 F.2d 791, 792 (CCPA 1971)); *In re Hiniker Co.*, 150 F.3d 1362, 1369 (Fed. Cir. 1998). In that regard, in order to be accorded substantial weight, there must be a nexus between the merits of the claimed invention and the evidence of secondary considerations. *In re GPAC Inc.*, 57 F.3d 1573, 1580 (Fed. Circ. 1995). "Nexus" is a legally and factually sufficient connection between the objective evidence and the claimed invention, such that the objective evidence should be considered in determining nonobviousness. *Demaco Corp. v. F. Von Langsdorff Licensing Ltd.*, 851 F.2d 1387, 1392 (Fed. Cir. 1988). The burden of showing that

there is a nexus lies with Alarm.com. *Id.*; *see also In re Paulsen*, 30 F.3d 1475, 1482 (Fed. Cir. 1994).

In this interference, Alarm.com argues non-obviousness based on what Alarm.com characterizes as "industrial skepticisms." In support of these arguments, Alarm.com relies on Dr. Malek (Ex. 2004) to provide testimony of non-obviousness because: (1) the choice of whether a mobile application should be developed as a native application or a web application was difficult and the tradeoffs between the two design choices were not readily understood by those skilled in the art; and (2) such skepticisms would have deterred a person of ordinary skill in the art to develop a native mobile device monitoring application. Paper 66, pp. 16–17 (citing Ex. 2004, ¶¶ 85–90). In particular, Dr. Malek directs us to several online articles written from several bloggers in the field of mobile software, including:

(1) Michael Mace who wrote in his own blog dated February 2008:

> [T]he business of making native apps for mobile devices is dying, crushed by a fragmented market and restrictive business practices. The problems are so bad that the mobile web, despite its many technical drawbacks, is now a better way to deliver new functionality to mobiles.

Ex. 2004, ¶ 86 (citing Ex. 2035 "Mobile applications, RIP," at http://mobileopportunity.blogspot.com/2008/02/mobile-applications-rip.html");

(2) Mike Rowehl, a well-known entrepreneur in the area of mobile computing, and founder and Chief Technology Officer of Metaresolver Inc., who wrote in a blog dated February 2008 that he agreed with Michael Mace's blog:

> The overall statement from Michael I agree with however: If you're a mobile developer, you should consider stopping native app development and shifting to a mobile-optimized website.

Ex. 2004, ¶ 87 (citing Ex. 2035 "Native Mobile Apps vs Mobile Web Apps," at http://www.thisismobility.com/blog/2008/02/25/native-mobile-apps-vs-mobile-web-apps/);

(3) Carlo Longino who wrote in a blog dated February 2008 that he also agreed with some aspects of Michael Mace's blog:

> I've been thinking a lot lately about the merits of mobile native development compared to mobile web development. Native mobile development is so complex and fraught with so many pitfalls, and that situation doesn't look like it's changing much, despite the advances many handset manufacturers and platform providers trumpet. Myriad technical issues remain, while the difficulty in establishing a business model persists. *Obviously this isn't a zero-sum game; there are plenty of instances where native apps make a lot more sense than web apps or services* (or are the only way to tackle a problem). But are those instances becoming more rare? And will the best mobile devices in the future — in terms of development platforms — just be the ones with the best browser?

Ex. 2004, ¶ 88 (citing Ex. 2036 "Sounding the Death Knell for Native Mobile Apps," at http://mobhappy.com/blog1/2008/02/25/sounding-the-death-knell-for-native-mobile-apps/) (emphasis added); and

(4) Dean Bubley, the founder of Disruptive Analysis, an independent technology industry analyst and consulting firm, who wrote in a blog dated February 2008 that he agreed with some parts of Michael Mace's blog:

> In general, I agree. Barcelona was full of widgets & web services, and I've been telling my handset software customers for some years that they should be working on the best browser implementations they can….
>
> I don't think the situation is quite that clear-cut though, and that *there will be plenty of reasons to continue using native apps on smartphones, together with other virtual machines and on-device portals like Java, Flash, BREW and SurfKitchen*…Bottom line – I

> totally agree with Michael that web-based applications are becoming much more important relative to 'installed' mobile apps. But I think it's a little early for the obituary, deeply amusing though it is.

Ex. 2004, ¶ 89 (citing Ex. 2037 "Standalone Mobile Apps vs Web Apps on Mobile," at http://disruptivewireless.blogspot.com/2008/02/standalone-mobile-apps-vs-web-apps-on.html/) (emphasis added).

Dr. Malek further testified:

> [T]he decision of developing a mobile app as a native application versus a web application was anything but obvious before the filing of the '694 patent. In fact, many of those skilled in the art felt that native mobile applications were not going to be the future of mobile computing, while many remained skeptical of the proper mobile application development approach.

Ex. 2004, ¶ 90.

Based on Dr. Malek's testimony, Alarm.com argues the choice of developing a native mobile device monitoring application in the Alarm.com '694 patent would have not been obvious to a person of ordinary skill in the art. Paper 66, p. 17.

We do not find Alarm.com's arguments persuasive. Nor do we find Mr. Malek's testimony credible on these points. As expressly recognized by Carlo Longino, "there are plenty of instances where native apps make a lot more sense than web apps or services." Ex. 2036. Likewise, Dean Bubley also acknowledges "there will be plenty of reasons to continue using native apps on smartphones, together with other virtual machines and on-device portals like Java, Flash, BREW and SurfKitchen.." Ex. 2037. For example, because of the success of Apple iPhones and the Apple Store in late 2008 and the competition from other smartphone manufactures, such as Samsung Electronics, LG, HTC, Sony and Motorola running on Android operating system (OS) based on the Linux kernel

developed by Google, many software developers became interested to develop all types of "native applications" for Apple iOS platform as well as other mobile device platforms such as Blackberry, Google Android, and Windows Mobile. *See* Ex. 1049 ("Apple Has Sold 450,000 iPads, 50 Million iPhones To Date"); and Ex. 1050 ("iPhone Overtaken by Android in the US"). One example of such software developers included iControl's own efforts to develop iControl's own "native mobile device monitoring applications" (Ex. 1010) as a commercial alternative for iControl's integrated security system disclosed by iControl '365 application (FF 25–26). *See* iControl Opposition 1 (Paper 144) at 16:13–17:4.

In view the differences between "native applications" and "web applications" and the success of Apple iPhones and Apple Store in late 2008 and the competition from other smartphone manufacturers, we agree with iControl that the choice of developing a native mobile device monitoring application in the Alarm.com '694 patent would have been obvious to those skilled in the art. *See* iControl Opposition 1 (Paper 144) at 16:13–17:4. Accordingly, we agree with iControl that the evidence of secondary considerations support a conclusion that Alarm.com's claims are obvious in view of iControl's claims.

For these reasons, we conclude that Alarm.com has failed to meet its burden of proof to establish that there is no interference-in-fact between Alarm.com's claims and iControl's claims. Accordingly, Alarm.com Motion 1 (Paper 66) is *denied*.

V. ALARM.COM MOTION 3 (PAPER 68) FOR DESIGNATING CLAIMS 2, 7, 13, 22, 27, 33, 42, 47, and 53 AS NOT CORRESPONDING TO THE COUNT

Alarm.com Motion 3 (Paper 68) seeks to designate Claims 2, 7, 13, 22, 27, 33, 42, 47, and 53 of Alarm.com '694 patent as *not* corresponding to the Count. Paper 68, pp. 1–18.

> A claim corresponds to a count if the subject matter of the count, treated as prior art to the claim, would have anticipated or rendered obvious the subject matter of the claim.

37 C.F.R. § 41.207(b)(2).

Alarm.com, as the moving party, bears the burden of proof to establish entitlement to the relief requested. 37 C.F.R. § 41.121(b).

To prevail in its motion, Alarm.com must demonstrate by a preponderance of the evidence that each of the subject matter of the claims it seeks to designate as not corresponding to the Count would not have been obvious when considered in view of the subject matter of the Count (iControl's claims).

Alarm.com identifies three features recited in Claims 2, 7, 13, 22, 27, 33, 42, 47, and 53 of Alarm.com '694 patent that allegedly distinguish from the Count and other applicable prior art.

For example, Alarm.com Claims 2, 22, and 42 depend from Claims 1, 21, and 41, respectively, recite:

> [S]ynchronizing, *over a short range wireless communication protocol*, with at least one component of the monitoring system located at the property such that the mobile device is able to exchange, directly with the at least one component of the monitoring system located at the property over the short range wireless communication protocol, data communications descriptive of sensor events detected by the monitoring system at the property.

Paper 11, pp. 3–15; Ex. 2001, Claims 2, 22, and 42 (emphasis added).

Alarm.com acknowledges the 802.11 short range wireless standard and home wireless networks were known by the invention of Alarm.com '694 patent. Paper 68, pp. 7–11 (citing Ex. 2003, Exhibit A, p. 3). However, Alarm.com relies on testimony from Dr. Malek to support an argument that the mere existence of the 802.11 short range wireless standard and home wireless networks would not have led one skilled in the art to modify the subject matter of the Count to incorporate features of Alarm.com Claims 2, 22, and 42. *Id*. at 8 (citing Ex. 2004, ¶ 94). According to Dr. Malek, a typical home wireless network that uses the 802.11 standard utilizes an access point (AP) that manages client devices connected to the home wireless network. As such, the access point (AP) synchronizes with the client devices and data communications exchanged in the home wireless network are routed through the access point (AP), rather than directly between the client devices connected to the home wireless network. *Id*. at 8–9 (citing Ex. 2004 ¶¶ 95–96). In other words, the mobile device can only communicate, via the access point (AP), and cannot communicate directly with a component of the monitoring system as recited in Alarm.com Claims 2, 22, and 42. Accordingly, Alarm.com argues the subject matter of the Count in view of the 802.11 short range wireless standard and home wireless networks raised by iControl would not have rendered obvious the features of Alarm.com Claims 2, 22, and 42 and, as such, Claims 2, 22, and 42 should be designated as *not* corresponding to the Count. *Id*. at 10.

We are not persuaded by Alarm.com's arguments. Nor do we find Dr. Malek's testimony credible on this point. First, as correctly recognized by iControl, Alarm.com's arguments are predicated upon an incorrect premise that Alarm.com's mobile device can communicate directly with associated devices (e.g., sensors or detectors) on a monitoring system without any access point (AP). iControl Opposition 3 (Paper 146), pp. 3–7.

For example, Alarm.com's '694 patent describes:

> The one or more mobile devices 140, 150 communicate with and receive monitoring system data from the monitoring system control unit **110** using the communication link **138.** For instance, the one or more mobile devices **140, 150** may communicate with the monitoring system control unit **110** using various local wireless protocols such as wifi, Bluetooth, zwave, zig bee, HomePlug (ethernet over powerline), or wired 10 protocols such as Ethernet and USB, to connect the one or more mobile devices **140, 150** to local security and automation equipment. The one or more mobile devices **140, 150** may connect locally to the monitoring system and its sensors and other devices. The local connection may improve the speed of status and control communications because communicating through the network **105** with a remote server (e.g., the monitoring application server **160)** may be significantly slower.
>
> Although the one or more mobile devices **140, 150** are shown as communicating with the monitoring system control unit **110,** the one or more mobile devices **140, 150** may communicate directly with the sensors and other devices controlled by the monitoring system control unit **110.** In some implementations, the one or more mobile devices **140, 150** replace the monitoring system control unit **110** (e.g., the main security/automation control panel) and perform the functions of the monitoring system control unit **110** for local monitoring and long range/offsite communication.
>
> In some examples, the monitoring system may include one or more local components at the property that are configured to communicate directly with the native mobile device monitoring application. In these examples, the one or more local components may include a control panel (e.g., a security system control panel) that is configured to communicate directly with the native mobile device monitoring application and/or sensors that are configured to communicate directly with the native mobile device monitoring application.

Ex. 1001, 6:3–28, 10:3–9.

As correctly pointed out by iControl, Alarm.com ’694 patent also teaches the use of an access point (AP) in the form of a “control panel (e.g., a security system control panel)” to synchronize with a “native mobile device monitoring application” as required by a home wireless network that uses the 802.11 standard. iControl Opposition (Paper 146) at 4:14–16 (citing Ex. 1043, ¶ 301).

Second, we note that obviousness under 35 U.S.C. § 103(a) is not a rigid concept. In such an obviousness analysis, it is not necessary to find precise teachings directed to the specific subject matter claimed because inferences and creative steps that a person of ordinary skill in the art would employ can be taken into account. *See KSR*., 550 U.S. at 418. In this regard, "[a] person of ordinary skill is also a person of ordinary creativity, not an automaton." *Id*. at 421.

Consideration should be given to what the combined teachings, knowledge of one of ordinary skill in the art, and the nature of the problem to be solved as a whole would have suggested to those of ordinary skill in the art (*see In re Keller*, 642 F.2d 413, 425 (CCPA 1981)).

In that regard, the Supreme Court has indicated that:

> [It is error to] assum[e] that a person of ordinary skill attempting to solve a problem will be led only to those elements of prior art designed to solve the same problem.... Common senses teaches . . . that familiar items may have obvious uses beyond their primary purposes, and in many cases a person of ordinary skill will be able to fit the teachings of multiple patents together like pieces of puzzle.

KSR 55 U.S. at 420 (citation omitted).

In this interference, we find the subject matter of Alarm.com’s claims 2, 22, and 42 is nothing more than “[t]he combination of familiar elements according to known methods” that do “no more than yield predictable results” when considered

in light of the Count. *KSR*, 550 U.S. at 415–16. In particular, the Supreme Court has explained:

> When there is a design need or market pressure to solve a problem and there are a finite number of identified, predictable solutions, a person of ordinary skill in the art has good reason to pursue the known options within his or her technical grasp. If this leads to the anticipated success, it is likely the product not of innovation but of ordinary skill and common sense.

KSR, 550 U.S. at 402–03.

Alarm.com has not presented sufficient evidence that an artisan would not have found these features obvious, in light of the Count, and other applicable prior art discussed *supra*, to enable a mobile device to exchange directly with associated devices (e.g., sensors and detectors) of the monitoring system located at the premise (home or office) over a short range wireless communication protocol. A person of ordinary skill in the art would have appreciated that such features would improve access to sensor events detected by the monitoring system at the premise, as required by the 802.11 short range wireless standard and home wireless networks.

Likewise, Alarm.com has not presented sufficient evidence or argument that alleged distinguishing features of Alarm.com Claims 2, 22, and 42 would have been "uniquely challenging or difficult for one of ordinary skill in the art" or otherwise beyond the level of an ordinarily skilled artisan and "represented an unobvious step over the prior art." *See Leapfrog Enters., Inc. v. Fisher-Price, Inc.*, 485 F.3d 1157, 1161-62 (Fed. Cir. 2007).

Turning now to Alarm.com Claims 7, 27, and 47, which depend from Claims 1, 21, and 41, respectively, and which further recite:

> the monitoring system is configured to perform operations comprising:

> tracking one or more characteristics of the mobile device that operates the native mobile device monitoring application;
>
> analyzing the tracked one or more characteristics with respect to a set of one or more rules;
>
> determining whether to perform an operation related to the tracked one or more characteristics based on the analysis; and
>
> performing the operation related to the tracked one or more characteristics in response to a determination to perform the operation.

Paper 11, pp. 3–15; Ex. 2001, Claims 7, 27, and 47.

Alarm.com acknowledges the scope of the prior art includes many mobile devices that perform the operations, including tracking battery power based on rules and thresholds. Paper 68, pp. 11–16 (citing Ex. 2003, Exhibit A, pp. 7–8). Nevertheless, Alarm.com relies on testimony from Dr. Malek to support an argument that: (1) mobile devices were generally thought to be useful extensions of a monitoring system that enable remote delivery of monitoring system information and remote control over monitoring system operations; (2) mobile devices were certainly seen as important for remote interaction with monitoring systems, but not seen as essential components of monitoring systems and, as such, (3) one skilled in the art would not have perceived a need to configure a monitoring system to track one or more characteristics of the mobile device that operates the native mobile device monitoring application, analyze the tracked one or more characteristics with respect to a set of one or more rules, determine whether to perform an operation related to the tracked one or more characteristics based on the analysis, and perform the operation related to the tracked one or more characteristics in response to a determination to perform the operation, as recited in Alarm.com Claims 7, 27, and 47. *Id*. at 12 (citing Ex. 2014 ¶¶ 116–118).

iControl responds that: (1) a mobile device is an essential component rather than optional component as alleged by Alarm.com; and (2) U.S. Patent No. 7,894,807 issued to Drennan (Ex. 1014) teaches, for example: (i) "tracking one or more characteristics of the mobile device" in the form of location information of the mobile device; (ii) "analyzing the tracked one or more characteristics with respect to a set of one or more rules" in the form of "a set of smart options or learning preferences" for the location information; (iii) "determining whether to perform an operation related to the tracked one or more characteristics based on the analysis" in the form of "a learning activation option, a training period option, and a dynamic profile update option; and (iv) "performing the operation related to the tracked one or more characteristics in response to a determination to perform the operation" in the form of "dynamically adjusting the user's routing preferences for cost, reliability or compliance with laws. Paper 146, pp. 7–11 (citing Ex. 1014, 3:11–47, 4:18–56. Based on such teachings, iControl responds that one skilled in the art would have combined the teachings of Drennan with iControl's claims to allow mobile device users to select the wireless or cellular network, for example to save money, for convenience or to comply with laws. *Id.* at 10 (citing Ex. 1014, 1:21–29, 2:2–9, and 4:18–39).

We are not persuaded by Alarm.com's arguments and agree with iControl's response. We conclude Alarm.com has not presented sufficient evidence that an artisan would not have found these features obvious, in light of the Count, and other applicable prior art discussed *supra*, to enable a monitoring system to track one or more characteristics of the mobile device that operates the native mobile device monitoring application in the manner recited in Alarm.com Claims 7, 27, and 47.

Lastly, Alarm.com Claims 13, 33, and 53 depend from Claims 1, 21, and 41, respectively, recite:

> the native mobile device monitoring application further includes instructions that, when executed by the mobile device, cause the mobile device to perform operations comprising:
> detecting an event related to the monitoring system;
> determining an operation needed to handle the detected event; and
> leveraging functionality, that is separate from the native mobile device monitoring application, of the mobile device in performing the determined operation.

Paper 11, pp. 3–15; Ex. 2001, Claims 13, 33, and 53.

Alarm.com acknowledges many mobile devices perform the operations, including receiving a text message describing a sensor event detected by a monitoring system. Paper 68, pp. 16–18 (citing Ex. 2003, Exhibit A, pp. 10–11). Nevertheless, Alarm.com argues that one skilled in the art would not have been led to move the detecting and handling performed by the monitoring system to the cell phone to send a text message to the cell phone as the cell phone would have no need to send a text message to itself. *Id*. at 16 (citing Ex. 2014 ¶¶ 226–228).

iControl responds Fig. 4 and related text of Alarm.com ’694 tracks the language of Claims 13, 33, and 53, and describes the system 100 performs the operations recited in those claims, not a mobile device. Paper 146, 12:19–21 (citing Ex. 1043, ¶ 322)

According to iControl, Alarm.com ’694 patent describes:

> “The system **100** detects an event related to the monitoring system (**410**). For instance, the system **100** may detect an alarm condition (e.g., a security breach) at a property. The system **100** also may detect a notification event that triggers consideration of whether a notification should be sent based on attributes sensed at the property. The system **100**

> further may detect requests to control the monitoring system as events. The system **100** may detect single events (e.g., a single contact sensor trigger) or detect a series or pattern of events (e.g., a pattern of contact sensor triggers, a motion sensor trigger, and an RFID tag identification)."

Id. at 12-13 (citing Ex. 1001, 15:50–63).

However, such features are disclosed, for example, by U.S. Patent 8,175,617 to Rodriguez (Ex. 1056) ("a smart phone that monitors the user's environment and automatically selects and undertakes operations responsive to visual and/or other stimulus.") *Id*. at 14 (citing Ex. 1056, 1:47–51, and Ex. 1043, ¶¶ 328).

We agree with iControl's response. Alarm.com Claims 13, 33, and 53 simply require a "native mobile device monitoring application" included in a mobile device to detect an event related to a monitoring system. Based on the teachings of Rodriguez, we find one skilled in the art would have considered Alarm.com Claims 13, 33, and 53 to have been rendered obvious by the subject matter of the Count in view of the teachings of Rodriguez.

For these reasons, we conclude that Alarm.com has failed to meet its burden of proof with respect to Claims 2, 7, 13, 22, 27, 33, 42, 47, and 53 of Alarm.com '694 patent. Accordingly, Alarm.com Motion 3 (Paper 68) is *denied*.

VI. CONCLUSION

Based on the record before us, we conclude that Alarm.com has not met its burden to show by the preponderance of evidence that: (1) Claims 62–79 of iControl's '365 application are unpatentable under 35 U.S.C. § 112, first paragraph, for lacking written description support; (2) the subject matter of Alarm.com's claims and the subject matter of iControl's claims do not interfere; and (3) Claims 2, 7, 13, 22, 27, 33, 42, 47, and 53 of Alarm.com '694 patent do not

correspond to the Count. As such, Alarm.com Motion 2 (Paper 67), Alarm.com Motion 1 (Paper 66) and Alarm.com Motion 3 (Paper 67) are *denied*.

As a result of the above decisions, and in light of Alarm.com's failure to file its own Priority Statement and to contest priority (Pape 193, p. 3), judgment will be entered against Alarm.com.

VII. ORDER

For the reasons discussed above, it is:

ORDERED that Alarm.com Motion 2 (Paper 67) alleging lack of written description support under 35 U.S.C. § 112, first paragraph, is *denied*;

FURTHER ORDERED that Alarm.com Motion 1 (Paper 66) for no interference-in-fact between Claims 1–60 of Alarm.com's involved patent, U.S. Patent No. 8,350,694 (Alarm.com '694 patent) and Claims 62–79 of iControl's involved application 13/311,365 (iControl '365 application) is *denied*;

FURTHER ORDERED that Alarm.com Motion 3 (Paper 67) for designating Claims 2, 7, 13, 22, 27, 33, 42, 47, and 53 of Alarm.com '694 patent as not corresponding to the Count is *denied*;

FURTHER ORDERED that iControl Motion 1 (Paper 27) is *dismissed* as *moot*;

FURTHER ORDERED that since Alarm.com does not allege a date of invention prior to iControl, that judgment on the issue of priority will be awarded against Alarm.com; and

FURTHER ORDERED that Claims 1–60 of Alarm.com's involved patent (Alarm.com '694 patent) will be cancelled in a separate paper.

/Hung H. Bui/
Administrative Patent Judge

cc:

Attorney for Junior Party – **Alarm.com**

W. Karl Renner, Esq.
Jeremy J. Monaldo, Esq.
Fish & Richardson P.C.
renner@fr.com
monaldo@fr.com

Attorney for Senior Party – **iControl Networks, Inc**.

Mark A. Lauer, Esq.
Richard L. Gregory, Jr., Esq.
Thomas W. Lathram, Esq.
Mark@SiliconEdgeLaw.com
Rick@IPRlaw.com
Tom@SiliconEdgeLaw.com