[DO NOT PUBLISH]

IN THE UNITED STATES COURT OF APPEALS

FOR THE ELEVENTH CIRCUIT

No. 15-11893

D.C. Docket No. 1:11-cv-02278-WSD

EARTHCAM, INC.,
a Delaware corporation,

Plaintiff - Counter
Defendant - Appellant,

versus

OXBLUE CORPORATION,
a Georgia corporation,
CHANDLER MCCORMACK,
Individually,
JOHN PAULSON,
Individually,
BRYAN MATTERN,
Individually,

Defendants - Counter
Claimant - Appellees,

RICHARD P. HERMANN, II,

Defendant - Appellee.

Appeal from the United States District Court
for the Northern District of Georgia

(July 27, 2017)

Before ED CARNES, Chief Judge, JORDAN, Circuit Judge, and SMITH,[*] District Judge.

PER CURIAM:

EarthCam, Inc., appeals the summary judgment entered in favor of OxBlue Corporation, Chandler McCormack, and Bryan Mattern (collectively known as the "OxBlue Defendants"), and Richard Hermann. EarthCam contends that the district court erred by (1) granting summary judgment on its trade secrets misappropriation claim against the OxBlue Defendants on grounds they allegedly never raised; (2) concluding that it had failed to assert a claim for injunctive relief; (3) granting summary judgment on its claim of unauthorized computer access despite a genuine issue over whether the OxBlue Defendants had accessed its computer system without or in excess of authorization; and (4) granting summary judgment on its trade secrets misappropriation claim against Mr. Hermann. EarthCam also appeals the district court's denial of its motion to reopen forensic discovery, arguing that it

[*] Honorable C. Lynwood Smith, Jr., United States District Judge for the Northern District of Alabama, sitting by designation.

should be allowed to ascertain whether certain forensic information was withheld and altered.

Following a review of the record and the parties' briefs, and with the benefit of oral argument, we affirm.

I

We exercise plenary review over a district court's grant of summary judgment. *See Moton v. Cowart*, 631 F.3d 1337, 1341 (11th Cir. 2011). In doing so, we draw all inferences and review all of the evidence in the light most favorable to the non-moving party. *Id.* The party moving for summary judgment bears the burden of demonstrating that there is no genuine dispute of any material fact and that it is entitled to judgment as a matter of law. *Id.* If the evidence supporting the nonmoving party is merely colorable or not significantly probative, summary judgment may be granted. *See Anderson v. Liberty Lobby, Inc.*, 477 U.S. 242, 249–50 (1986).

We review the district court's denial of a motion to reopen discovery for abuse of discretion. *See Artistic Entm't, Inc. v. City of Warner Robins*, 331 F.3d 1196, 1202 (11th Cir. 2003).

II

EarthCam raises five issues in its initial brief. We address the specific arguments advanced by EarthCam and nothing more. *See Access Now, Inc. v. Sw.*

Airlines Co., 385 F.3d 1324, 1330 (11th Cir. 2004) ("[A] legal claim or argument that has not been briefed before the court is deemed abandoned and its merits will not be addressed."). Because we write for the parties, we set out only what is necessary to explain our decision.

A

EarthCam argues that the district court erroneously granted summary judgment on its trade secrets misappropriation claim against the OxBlue Defendants under the Georgia Trade Secrets Act, O.C.G. § 10-1-760 *et seq*. Specifically, with respect to two instances of alleged misappropriation (the so-called "brute force attack" and the "OxBlue 3019" file), EarthCam contends that the district court's order was based on arguments not raised by the OxBlue Defendants: (1) that the information obtained in the 2006 brute force attack lacked economic value; and (2) that the data in the OxBlue 3019 file was not a trade secret. The lack of notice, EarthCam contends, deprived it of an opportunity to respond, in violation of Federal Rule of Civil Procedure 56(f).

The district court's order and the motion filed by the OxBlue Defendants belie EarthCam's cry of summary judgment by ambush. In the portion of the summary judgment motion attacking EarthCam's trade secrets misappropriation claim, the OxBlue Defendants maintained that EarthCam had to prove "(a) the existence of a trade secret[ ] (b) that was misappropriated." D.E. 228-1 at 7. After

defining a "trade secret" as information that derives economic value from not being generally known to others and that is the subject of reasonable efforts to keep secret, *see id.* at 8 (citing O.C.G. § 10-1-761(4)), the OxBlue Defendants generally argued that none of the information EarthCam identified—including information obtained in the 2006 brute force attack and the OxBlue 3019 data, *see* D.E. 228-20 ¶¶ 2, 5, 8—constituted "trade secrets" because the information was "public," belonged to third parties, or was general customer or business information. *See* D.E. 228-1 at 7.

If this general assertion were not enough, the OxBlue Defendants then lodged specific attacks against the 2006 brute force attack and the OxBlue 3019 data. With respect to the brute force attack, the OxBlue Defendants maintained that any information they "scraped" from EarthCam's website was regularly made public by EarthCam, often for marketing purposes. *See id.* at 9–10. And information intentionally publicized by EarthCam could not have derived its economic value from secrecy, as required by § 10-1-761(4). *See id.* The district court agreed with this argument, ruling against EarthCam in part because it "ha[d] not presented any evidence to support that the information gathered in [the brute force attack of] 2006 even potentially derived economic value from not being generally known." D.E. 292 at 31. The district court, in other words, based its decision in part on an argument explicitly raised by the OxBlue Defendants.

The OxBlue Defendants similarly contested OxBlue 3019's status as a trade secret, insisting throughout the motion that EarthCam had failed to identify what exactly in the OxBlue 3019 file constituted a trade secret. *See* D.E. 228-1 at 11–12 (arguing that none of the information Mr. Hermann allegedly gave to OxBlue, including the OxBlue 3019 file, was a trade secret), 12 n.13 ("[EarthCam] has not specified what information contained [in OxBlue 3019] is a 'trade secret.'") (citing the OxBlue Defendants' statement of undisputed material facts in support of their renewed motion for summary judgment, D.E. 228-2).

In sum, we conclude that EarthCam was sufficiently on notice that it had to respond to the contention that the information obtained in the 2006 brute force attack and the OxBlue 3019 data were not trade secrets under the GTSA. Because we reject the only two grounds raised by EarthCam for reversing the summary judgment granted on its trade secrets claim against the OxBlue Defendants, *see* Br. of Appellant at 12–13, we affirm that portion of the district court's order.

B

According to EarthCam, the OxBlue Defendants moved for summary judgment solely as to the damages portion of its GTSA claim, so EarthCam responded in part by arguing that it also sought an injunction prohibiting future use or disclosure of trade secrets. The district court allegedly refused to consider this argument on the ground that it was a "newly raised claim." Br. of Appellant at 23

(quoting D.E. 292 at 35). EarthCam argues that the district court was incorrect because the request for injunctive relief had previously appeared in the second amended complaint. *See* D.E. 117.

The OxBlue Defendants dispute EarthCam's characterization of the district court's decision. *See* Br. of Appellees at 27–30. But even assuming everything played out as EarthCam says it did, reversal is unwarranted because this issue is mooted by our affirmance of the district court's grant of summary judgment on the merits of the GTSA claim against the OxBlue Defendants. By failing on the merits, EarthCam cannot obtain any relief whatsoever under the GTSA.

C

EarthCam contends that the OxBlue Defendants violated the Computer Fraud and Abuse Act, 18 U.S.C. § 1030, in May of 2011 when they accessed the account webpage of an EarthCam customer, Forest City Ratner. The CFAA prohibits, among other things, "intentionally access[ing] a computer without authorization or [in excess of] authorized access, and . . . obtain[ing] . . . information." § 1030(a)(2)(C). EarthCam says that OxBlue personnel captured and downloaded screenshots of the graphical user-interface running on FCR's

account webpage. *See* D.E. 255-4 at 4 ¶ 12 (describing the screenshots allegedly captured by OxBlue personnel).[1]

It turns out (and it is undisputed), however, that a man by the name of Chip Foley, who was with FCR, had asked the OxBlue Defendants to troubleshoot certain issues FCR was having with EarthCam equipment and had provided OxBlue personnel his account login credentials to do so. *See* D.E. 255-1 at 47–51 ¶¶ 11–23, at 66–67 ¶¶ 93–98. The district court found no CFAA violation given this evidence, reasoning that the OxBlue Defendants had accessed the account webpage with FCR's authorization. The district court also concluded that nothing in the End-User License Agreement applicable to FCR's account prohibited FCR from sharing its login credentials, and that the OxBlue Defendants did not knowingly violate the EULA's terms because there was "no evidence that the OxBlue Defendants were familiar with the EULA, or that the OxBlue Defendants viewed the EULA when they accessed FCR's EarthCam account [on May 20 and 21, 2011]." D.E. 292 at 38.

EarthCam does not dispute that the OxBlue Defendants accessed the account webpage under FCR's authorization, and that the EULA did not prohibit FCR from sharing its login credentials. Even so, EarthCam claims summary judgment was incorrectly granted for two reasons.

[1] This is the only alleged instance of unauthorized access at issue on appeal. *See* Br. of Appellant at 25–26 & n.27 (relying on the FCR access as the basis for the CFAA claim).

First, EarthCam argues that the access of the OxBlue Defendants was without authorization because, in order to log on to FCR's account, they knowingly circumvented EarthCam's security measures aimed at blocking OxBlue personnel from accessing its webpage. *See* Br. of Appellant at 27. There is evidence in the record that Mr. McCormack acknowledged that EarthCam was blocking OxBlue's IP address and that OxBlue personnel got around this by masking their IP address. The OxBlue Defendants maintain, however, that this argument is a complete nonstarter because it was never raised below. *See* Br. of Appellees at 34 & n.21. EarthCam, in response, urges us not to disregard OxBlue's furtive evasion of its security measures, arguing that it properly preserved that argument by presenting the facts to the district court in its response to the OxBlue Defendants' motion for summary judgment. *See* Reply Br. at 17–18 & n.8.

We agree with the OxBlue Defendants that EarthCam failed to preserve this argument. EarthCam briefly addressed the OxBlue Defendants' CFAA arguments at summary judgment in Part III.B of its response. *See* D.E. 255 at 21–22. That portion of the response made only two arguments: (1) that the OxBlue Defendants' access was unauthorized, even though it was under the auspices of FCR's authority, because it violated the EULA; and (2) that there was sufficient evidence in the record demonstrating that OxBlue personnel had previously viewed and

accepted the EULA. *See id*. The IP-masking argument, as a basis for CFAA liability, is nowhere to be found. Because EarthCam failed to press that below, we will not consider it now. *See Resolution Trust Corp. v. Dunmar Corp.*, 43 F.3d 587, 599 (11th Cir. 1995).

Second, EarthCam contends that there is a genuine dispute over whether the OxBlue Defendants were "'presumably familiar with the terms' of the EULA" applicable to FCR's account, Br. of Appellant at 30 (quoting *State Analysis, Inc. v. Am. Fin. Servs. Assoc.*, 621 F. Supp. 2d 309, 316 (E.D. Va. 2009)), such that they can be said to have knowingly violated the EULA's prohibition against "downloading screenshots of EarthCam's software." *Id.* At the end of the day, we are not persuaded.

EarthCam relies on *State Analysis* for the proposition that knowingly violating the terms of a licensing agreement renders access unauthorized. *See* Br. of Appellant at 30. But that case is not exactly on point. The licensing agreement in *State Analysis* prohibited licensees from sharing their login credentials. *See State Analysis*, 621 F. Supp. 2d at 316 ("[The plaintiff-licensor] has pled that under the terms of their contract, only clients were authorized to use [its] subscription services . . . ."). And the defendant unquestionably knew this because it had once been a client of the licensor's and subject to the same licensing agreement. *See id.*

The district court concluded that, because the defendant knew of this prohibition, it could not "hide" behind any authorization derived from the licensee. *See id.*

FCR, on the other hand, was not prohibited from sharing its login credentials. In fact, FCR could have made its account webpage public if it wished. *See* D.E. 255-1 at 46 ¶ 5 (citing D.E. 255-4 at 8 ¶ 28). So, in contrast to *State Analysis*, where the third-party access was unauthorized from inception by the licensing agreement, this case presents the much more difficult question of whether a person who otherwise has authorized access to a computer (as the OxBlue Defendants undoubtedly had when FCR gave them permission to access its account) exceeds authorization if he or she uses that access in a way that contravenes *any* policy or term of use governing the computer in question (here, the EULA's prohibition against downloading screenshots, *see* Br. of Appellant at 30).

The CFAA does not define the phrase "without authorization," but it defines "exceeds authorized access" as "to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter." 18 U.S.C. § 1030(e)(6). We have, in one published opinion, expounded on what it means to "exceed authorized access." *See United States v. Rodriguez*, 628 F.3d 1258 (11th Cir. 2010). In *Rodriguez*, the defendant had access, through his work as a TeleService representative for the Social

Security Administration, to certain SSA databases containing sensitive personal information. SSA policy authorized the defendant's access to the databases only for official business purposes. The defendant knew this, but chose to access the database and obtain information for nonbusiness reasons. *See id.* at 1263. We concluded that the defendant's access, which had been in furtherance of nonbusiness purposes, exceeded the authorization the SSA had given him, and affirmed his conviction under the CFAA. *See id.* at 1263–64.

Although it is not entirely clear, one of the lessons from *Rodriguez* may be that a person exceeds authorized access if he or she uses the access in a way that contravenes any policy or term of use governing the computer in question. So, assuming that the OxBlue Defendants actually violated the EULA, there is an argument that downloading the screenshots "exceeded authorized access" under *Rodriguez*.[2]

Even if this is a valid reading of *Rodriguez*, there is insufficient evidence that the OxBlue Defendants *knowingly* violated the EULA, which is (and has been) EarthCam's theory of CFAA liability and, therefore, the only argument we are

[2] We decided *Rodriguez* in 2010 without the benefit of a national discourse on the CFAA. Since then, several of our sister circuits have roundly criticized decisions like *Rodriguez* because, in their view, simply defining "authorized access" according to the terms of use of a software or program risks criminalizing everyday behavior. *See United States v. Valle*, 807 F.3d 508, 527 (2d Cir. 2015); *WEC Carolina Energy Sols. LLC v. Miller*, 687 F.3d 199, 206 (4th Cir. 2012); *United States v. Nosal*, 676 F.3d 854, 862–63 (9th Cir. 2012) (en banc). Neither the text, nor the purpose, nor the legislative history of the CFAA, those courts maintain, requires such a draconian outcome. We are, of course, bound by *Rodriguez*, but note its lack of acceptance.

obligated to address on appeal. *See Access Now*, 385 F.3d at 1330. Under that theory, we think that EarthCam's contention that the OxBlue Defendants "presumably" knew the terms of the EULA governing FCR's license is too much of an inferential leap to withstand summary judgment.

Everyone agrees that OxBlue personnel did not encounter and accept the EULA when they troubleshot FCR's issues on May 20 and 21, 2011. *See* Reply Br. at 18. But EarthCam says that OxBlue personnel had done so before, as evidenced by log files showing that users with OxBlue IP addresses had "viewed and accepted the EULA restrictions 'numerous' times between May 2010 and May 2011." Br. of Appellant at 28 (quoting D.E. 255-4 at 5–6 ¶¶ 17–18). And so, the argument goes, since OxBlue personnel had accepted the EULA in the past while accessing other users' accounts, they must have known that the EULA applied to FCR's account on May 20 and 21, 2011. *See* Reply Br. at 18 (conceding that the relevant "intrusion" occurred on May 20 and 21, 2011, and that there is no direct evidence that OxBlue personnel accepted the EULA on those dates). *See also* D.E. 255-1 at 49 ¶ 19 (describing EarthCam's access onto FCR's account as the "May 2011 intrusion").

Bill Sharp, EarthCam's vice president of technology, explained how the EULA worked. He testified that all users with an EarthCam account must accept the EULA the very first time they log on to their accounts. *See* D.E. 255-19 at

147–48. EarthCam's system automatically prompts them. *See id.* After accepting it once, the system does not prompt users again unless there is a change in terms. *See id.* But there is no evidence that the OxBlue Defendants knew any of this. The log files, even in the light most favorable to EarthCam, only indicate that users with OxBlue's IP address had accepted the EULA in the past. *See* D.E. 255-1 at 48 ¶ 16. It is unclear whether the version those users accepted is the same version that applied to FCR's account on May 20 and 21, 2011. But even if it was the same version, nothing in the record indicates that the OxBlue Defendants knew that the EULA governing FCR's account was the same one they had previously accepted. It would not be odd, for instance, if the terms of the EULA varied by customer, depending on the customer's needs and bargaining power.

Unlike the surefire evidence establishing knowledge in *State Analysis*, EarthCam's assertion that the OxBlue Defendants had knowledge of the EULA's terms hinges on layers of inference. From the simple fact that users with an OxBlue IP address had previously accepted the EULA, EarthCam wants us to allow a jury to find that the OxBlue Defendants knew the specifics of the EULA governing FCR's account. In between those two points, however, are a string of inferences about EarthCam's knowledge, including knowing that every EarthCam customer was subject to an EULA, that all customers were all subject to the same EULA, and that there had not been a new version between logins. We believe this

too attenuated to create a jury question on knowledge. *See Salter v. Westra*, 904 F.2d 1517, 1525 (11th Cir. 1990) ("When inferences are built upon inferences, the probability of the last or ultimate inference is attenuated by each underlying inference.").

Accordingly, we affirm the district court's grant of summary judgment on EarthCam's CFAA claim.

D

EarthCam next argues that the district court erroneously granted summary judgment on its GTSA claim against Mr. Hermann. The district court made two rulings as to this particular claim. First, the district court found that EarthCam and Mr. Hermann had executed a general release on August 13, 2008, that now precluded EarthCam from relying on any pre-release conduct to substantiate its GTSA claim. Second, the district court analyzed the email correspondence between Mr. Hermann and the OxBlue Defendants after August 13, 2008, and concluded that none of the information exchanged constituted a trade secret. EarthCam does not challenge the district court's interpretation of the general release. *See* Br. of Appellant at 31. Instead, EarthCam only appeals the district

court's conclusion that none of the information Mr. Hermann allegedly provided to OxBlue in emails after August 13, 2008, constituted a trade secret.[3]

Under the GTSA, a plaintiff must prove that "(1) it had a trade secret and (2) the opposing party misappropriated the trade secret." *Camp Creek Hosp. Inns, Inc. v. Sheraton Franchise Corp.*, 139 F.3d 1396, 1410 (11th Cir. 1998). The GTSA defines trade secret as information that derives economic value from not being well known to others and is the subject of reasonable efforts to maintain its secrecy. *See* O.C.G. § 10-1-761(4). "Whether a particular type of information constitutes a trade secret is a question of fact." *Camp Creek*, 139 F.3d at 1410–11. *See also Outside Carpets, Inc. v. Indus. Rug Co.*, 228 Ga. 263, 267 (1971). That being said, we have "consistently held that conclusory allegations without specific

[3] In addition to the various emails exchanged after August 13, 2008, EarthCam also argues that Mr. Hermann gave the OxBlue Defendants trade secrets in a file called OxBlue 3019. The parties dispute exactly when the OxBlue Defendants obtained the 3019 file. EarthCam says it was in June of 2009, while the OxBlue Defendants contend that it was in July of 2008. *See* Br. of Appellant at 6; Br. of Mr. Hermann at 9. The date of the transfer is important because it determines whether the general release applies, such that EarthCam may rely on the 3019 file to substantiate its GTSA claim against Mr. Hermann.

EarthCam's theory on the date of the transfer stems from an email sent on June 19, 2009, in which Mr. Hermann asked Mr. McCormack for an FTP site to upload several files. FTP sites, according to EarthCam, are used to transfer large amounts of data. The 3019 file being a very large file, EarthCam argues that the "logical[ ] infer[ence]" is that Mr. Hermann transferred the 3019 file using the FTP site, in 2009. *See* Br. of Appellant at 6.

Yet again, EarthCam overreaches. On its face, the email does not reference the 3019 data. The capabilities of an FTP site tell us nothing about what the medium was actually used for. Making conclusions about the 3019 data, without more, is nothing more than sheer speculation. Mr. McCormack, in contrast, affirmatively testified that he acquired the 3019 file in 2008. *See* D.E. 256-33 at 373. In short, we agree with the district court that the June 19 email is not enough to create a jury question on whether the 3019 data was transferred in 2009.

supporting facts have no probative value for a party resisting summary judgment." *Bazemore v. Jefferson Capital Sys., LLC*, 827 F.3d 1325, 1333 (11th Cir. 2016) (internal quotation marks omitted).

The district court granted summary judgment after concluding that the emails only contained general information that Mr. Hermann had learned during his tenure with EarthCam. Information stored in an employee's mind, the district court explained, was not protected by the GTSA. *See Manuel v. Convergys Corp.*, 430 F.3d 1132, 1140 (11th Cir. 2005) (collecting Georgia cases holding that the GTSA does not prohibit a former employee from exploiting the knowledge he or she accumulated during the prior employment). EarthCam, citing several emails as evidence, argues that the district court incorrectly characterized the exchanges as information "in [Mr. Hermann's] head." Br. of Appellant at 32.

The debate over whether the information was truly in Mr. Hermann's head is a sideshow because, as the district court recognized, even if we agree that Mr. Hermann was not merely recalling general information from memory, EarthCam did not provide sufficient evidence demonstrating that the email correspondence after August 13, 2008, contained trade secrets. *See* D.E. 292 at 53 (describing the

email correspondence from 2009–2010 as suffering from the same flaw as the other evidence presented by EarthCam).[4]

Almost exclusively, EarthCam relies on an affidavit by Mr. Sharp to establish that the emails contained trade secrets. *See* D.E. 256-3. *See also* D.E. 256-1. His affidavit is littered with conclusory allegations, all following the same script. First, Mr. Sharp vaguely alleges that Mr. Hermann gave away some kind of information, such as EarthCam's "revenue sources and income model." D.E. 256-3 at 17 ¶ 54. Then, he labels the information a "proprietary trade secret." *Id.* at 16–18 ¶¶ 53–55, 58–62. And finally, instead of fleshing out what he means, Mr. Sharp flatly declares that the particular piece of information "was not publicly available and gave EarthCam a competitive advantage." *Id.* at 16–19 ¶¶ 53–62. This sort of conclusory labeling and bare recitation of a statutory definition is precisely the kind of evidence that we have held cannot withstand summary judgment. *See Bazemore*, 827 F.3d at 1333.

As an example of the circular nature of EarthCam's evidence, take an email sent by Mr. Hermann referencing EarthCam's use of timers in its solar system. *See* D.E. 230-21. The parties dispute whether this information is a trade secret. At summary judgment, Mr. Hermann argued that the information is not a trade secret

[4] For purposes of our review of EarthCam's GTSA claim against Mr. Hermann, these post-release emails are the only evidence EarthCam has left to substantiate its claim and survive summary judgment. Recall that EarthCam has abandoned a GTSA claim against Mr. Hermann based on pre-release misappropriation, and that we have agreed with the district court that no reasonable juror could find that the OxBlue 3019 file was transferred after the release.

because any purchaser of an EarthCam camera would know about the timer. To support his contention, Mr. Hermann cited the deposition of Mr. McCormack, in which he explained that the use of timers in these systems is "standard" and that OxBlue itself had an integrated timer for purposes of making its systems more efficient. *See* D.E. 230-1 at 4 ¶ 28 (citing D.E. 230-7 at 12). Mr. McCormack further explained that the timers themselves are made by a company called Dial, and that the integrated timer is provided by SunWize. *See* D.E. 230-7 at 13. If these factual allegations are true, then the information disclosed by Mr. Hermann is not protected because information available in the public domain, such as information sold to customers or known throughout the industry, does not constitute a trade secret. *See Roboserve, Ltd. v. Tom's Foods, Inc.*, 940 F.2d 1441, 1454 (11th Cir. 1991) (explaining that placing information in the public domain destroys any reasonable expectation of privacy and is not protected by Georgia law). Without a genuine dispute as to these facts, then, Mr. Hermann would be entitled to summary judgment on EarthCam's GTSA claim.

EarthCam responded by alleging, in relevant part, that Mr. Hermann "provide[d] OxBlue information that EarthCam considered confidential." D.E. 256-1 at 10. And it supported this allegation with a citation to its own statement of material facts that reads:

> On October 12, 2009, Hermann provided information EarthCam considered confidential on EarthCam's solar timer system and the

> way in which EarthCam received better run times and performance from their systems.

Id. at 33 ¶ 88. But allegations in a party's statement of material facts are themselves not evidence. *See* Fed. R. Civ. P. 56(c)(1)(A). Such statements require a foundation in the record. *See id.* The *only* record support cited by EarthCam was to the very same email at issue. *See* D.E. 256-1 at 33 ¶ 88 (citing Exhibit 45, D.E. 256-50); D.E. 256-50. That email tells us what Mr. Hermann communicated to Mr. McCormack, but it does not explain why the information is a trade secret, nor does it refute Mr. McCormack's testimony (cited by Mr. Hermann) that the timers were industry standard, that OxBlue's systems already used integrated timers, and that the timers were manufactured and provided by third-party vendors.

EarthCam's other allegations about the timer similarly fail to create a genuine dispute. Immediately after it asserted (with no evidentiary support) that the timer was "confidential," EarthCam repeated its usual incantation that the information on the timer "was not publicly available and gave EarthCam a competitive advantage." D.E. 256-1 at 33 ¶ 89. And, in support, it cites none other than Mr. Sharp's own verbatim recitation of this conclusory statement. *See id.* (citing Exhibit 3, D.E. 256-3, ¶ 61); D.E. 256-3 at 19 ¶ 61.

This exercise in tautology is not limited to the disclosure of the timer. Nearly every assertion on the information disclosed in the post-release emails eventually makes its way back to Mr. Sharp's affidavit. *See, e.g.*, D.E. 256-1 at

29–33 ¶¶ 61, 63, 67, 69, 71, 77, 79, 81, 83, 85, 89, 91. Declaring that something is confidential and a trade secret is not the same thing as providing evidence that the information (a) "is not commonly known by or available to the public," (b) "[d]erives economic value . . . from not being generally known," *and* (c) "[i]s the subject of efforts that are reasonable under the circumstances to maintain its secrecy." *See* O.C.G. § 10-1-761. And so, we agree with the district court that EarthCam has failed to provide sufficient evidence from which a reasonable juror could conclude that Mr. Hermann disclosed, in the email correspondence after August 13, 2008, EarthCam's trade secrets.

E

EarthCam appeals the denial of its motion to reopen discovery. According to EarthCam, it was entitled to reopen discovery because John deCraen, the OxBlue Defendants' computer forensic expert, violated the forensic investigation protocol the parties had agreed upon in several ways: first, by failing to turn over all of the 3019 data he encountered during his forensic analysis; second, for the 3019 data he did produce, by providing an incomplete image of the device that contained the data, which made it impossible for EarthCam's expert to determine what exactly was done with the data; and third, by not following and applying industry standard practices in his analysis. We conclude that the district court did not abuse its discretion in denying EarthCam's motion.

When a party fails to complete discovery in time, it may move to reopen discovery and the court may, "for good cause," grant the motion if the party shows that it failed "because of excusable neglect." Fed. R. Civ. P. 6(b)(1)(2). The Supreme Court has generally instructed courts to consider four factors in determining whether a party has shown excusable neglect: (1) the danger of prejudice to the nonmovant; (2) the length of the delay and its potential impact on judicial proceedings; (3) the reason for the delay, including whether it was within the reasonable control of the movant; and (4) whether the movant acted in good faith. *See Pioneer Inv. Servs. Co. v. Brunswick Assocs. Ltd. P'ship*, 507 U.S. 380, 395 (1993).

EarthCam bears significant responsibility for failing to complete forensic discovery within the original period prescribed by the district court. EarthCam filed this lawsuit on July 12, 2011, and discovery did not end until August 30, 2013, after several extensions by the district court. *See, e.g.*, D.E. 27; D.E. 189; D.E. 202. Forensic discovery was pursuant to an investigation protocol that the parties, together with a court-appointed computer forensic mediator, had negotiated and agreed upon. *See* D.E. 249-8. The OxBlue Defendants produced the information required by the protocol in May of 2013, but EarthCam did not move to reopen discovery until October 1, 2013.

Part of EarthCam's justification for the delay was that it did not know of several alleged shortcomings in the OxBlue Defendants' forensic production until it deposed Mr. deCraen. *See* D.E. 292 at 71. It is not entirely clear why EarthCam could not figure out the alleged shortcomings sooner, especially since it had already retained its own computer forensic expert, Jim Persinger. Mr. Persinger, at least as contemplated by the investigation protocol, played a significant role in reviewing Mr. deCraen's production. More importantly, as the district court pointed out, EarthCam chose to depose Mr. deCraen on the last day of discovery. *See id.* So even if a deposition was necessary, it was EarthCam's fault for not deposing him sooner.

Additionally, at the time of the motion, the OxBlue Defendants had already filed two fully-briefed motions for summary judgment. The district court had previously denied, without prejudice, the OxBlue Defendants' motion for summary judgment after it granted EarthCam's motion to expand discovery and designate Mr. Persinger (whom the district court allowed EarthCam to designate after the initial discovery period, *see* D.E. 189 at 10, 12–14) as its computer forensic expert witness. *See* D.E. 202 at 2 n.1. Like their first motion, the OxBlue Defendants' second motion would most likely have been rendered moot by additional discovery. In light of EarthCam's unjustified delay, it would have been prejudicial

to require the OxBlue Defendants to brief and file a *third* motion for summary judgment.

We also doubt EarthCam's contention that Mr. deCraen's performance was substandard. Mr. deCraen's forensic production was pursuant to a protocol that he crafted along with Mr. Persinger and a neutral court expert. Mr. deCraen's techniques, and any problems EarthCam may have had with them, could and should have been addressed upfront. Yet EarthCam never challenged, by way of a *Daubert* motion, Mr. deCraen's capabilities as an expert at any time before the district court. It cannot do so now in stoppage time.

Finally, try as it may to paint its request for additional discovery as a necessary byproduct of austere discovery orders, we are not convinced by EarthCam's arguments. Because the impact on judicial proceedings of extending discovery varies from case to case, district courts have considerable leeway in handling discovery matters. The district court in this case struck a careful balance between unwieldy discovery costs and the search for truth. It allowed considerable and lengthy forensic discovery of several computer devices that EarthCam believed to be involved in the alleged computer attacks. And it did so with the aid of both neutral and partisan experts (four computer forensic experts have worked on this case at one point or another), several of whom filed expert reports in this case.

On this record, and given the protracted nature of this litigation and the district court's thorough order, we do not find an abuse of discretion. *See Macklin v. Singletary*, 24 F.3d 1307, 1311 (11th Cir. 1994) (explaining that the abuse of discretion standard allows a "range of choice" for the district court as long as there is no "clear error of judgment") (citation and internal quotation marks omitted).

III

For these reasons, we affirm the district court's grant of summary judgment.

AFFIRMED.