United States Court of Appeals
For the First Circuit

No. 16-1049

JASON BOUDREAU,

Plaintiff, Appellant,

v.

STEVE LUSSIER; JOHN LUSSIER; STEVE SOREL; KEVIN PETIT; OFFICER KIM CARROLL; OFFICER NATHAN BAGSHAW; SERGEANT WELLER; CITY OF CRANSTON; CITY OF WARWICK; DONALD LUSSIER,

Defendants, Appellees,

OFFICER JAMES NEEDHAM,

Defendant.

APPEAL FROM THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF RHODE ISLAND
[Hon. Lincoln D. Almond, U.S. Magistrate Judge]

Before
Torruella, Lynch, and Barron,
Circuit Judges.

Patrick T. Roath, for appellant.

Douglas A. Giron, with whom Shechtman Halperin Savage, LLP was on brief, for appellees Steve Lussier, John Lussier, Donald Lussier and Steve Sorel.

Christopher E. Hultquist, with whom DeLuca & Weizenbaum Ltd. on brief, for appellees Officer Kim Carroll, Officer Nathan Bagshaw, Sergeant Weller, and City of Cranston.

Marc DeSisto, with whom Kathleen M. Daniels, and DeSisto Law LLC on brief, for appellees Kevin Petit, and City of Warwick.

August 21, 2018

TORRUELLA, **Circuit Judge**. Jason Boudreau worked for Automated Temperature Controls, Inc. (ATC), in Cranston, Rhode Island. His employers came to suspect that he was viewing child pornography at work. As a result, they covertly installed screenshot-capturing software on Boudreau's work computer, which confirmed these suspicions. This led them to contact law enforcement. To make a long story short -- a story we will explain in much greater detail below -- this culminated in Boudreau's arrest and plea of nolo contendere in state court to one count of possession of child pornography. Boudreau then brought a host of claims under 42 U.S.C. § 1983 and the Electronic Communications Privacy Act (ECPA), 18 U.S.C. § 2511, against the various individuals who participated in the events leading up to and following his arrest. The named defendants, now the appellees, included: ATC corporate president Steven Lussier, ATC co-owner John Lussier, and ATC information technology manager Steven Sorel (collectively, the "ATC Defendants); the City of Cranston and Cranston Police Department Officer Kim Carrol, Officer Nathan Bagshaw, and Sergeant Greg Weller (collectively, the "Cranston Defendants"); and the City of Warwick and Warwick Police Department detective Kevin Petit (collectively, the "Warwick Defendants").

The district court granted summary judgment in favor of the defendants on all of Boudreau's claims. Boudreau has appealed. We affirm.

I.

We view the facts in the summary judgment record in the light most favorable to Boudreau, and draw all reasonable inferences in his favor. See Mu v. Omni Hotels Mgmt. Corp., 882 F.3d 1, 3 (1st Cir. 2018).

A.

Boudreau worked for ATC from September 2009 to June 2011. At some point during the second week of June 2011, Boudreau asked Sorel to help recover email records that had been deleted from Boudreau's work computer. The file recovery software that Sorel employed compiled a list of "recoverable" files that had been deleted from that computer. This list included a number of pornographic movies and photos. Sorel brought this to Steven Lussier's attention. In response, Steven Lussier directed Sorel to install the screen-capture software System Surveillance Pro (SSP) on Boudreau's work computer. Sorel did so -- unbeknownst to Boudreau -- on June 16, 2011. SSP captures and saves screen-shots of whatever is being displayed on the monitor of the computer on which it is installed. Sorel configured SSP to take screenshots whenever the user of Boudreau's computer typed certain keywords, including, for example, "yahoo." Sorel also arranged for SSP to send these screenshots to an email account that he had set up specifically for that purpose.

On June 20, 2011, SSP captured screenshots of what Sorel -- who reviewed those screenshots two days later -- believed to be images of child pornography. The ATC Defendants conferred, and decided to contact law enforcement. On June 23, Steven Lussier delivered a USB drive containing the offending screenshots to Detective Kevin Petit of the Warwick Police Department. Detective Petit also requested to analyze Boudreau's work computer. So, the following morning, John Lussier and Sorel brought him that computer, and John Lussier signed a consent form for Detective Petit to search the computer. Detective Petit's ensuing search revealed numerous files containing child pornography.

John Lussier also mentioned to Detective Petit that ATC had provided a company laptop to Boudreau, and Detective Petit responded that he wanted to examine that laptop as well. That afternoon, Detective Petit spoke to John Lussier about Boudreau's company laptop again. John Lussier told Detective Petit that Boudreau was out golfing with Steven Lussier, but that he would be returning to ATC later on. During this conversation, Detective Petit also told John Lussier that he had become aware that Boudreau's driver's license had been suspended. Detective Petit then contacted Cranston Police Officer Nathan Bagshaw, relaying information about his investigation of Boudreau and that Boudreau would be driving back to ATC on a suspended license. Officer Bagshaw, Officer Kim Carrol, and Sergeant Gregg Weller then

dispatched to ATC headquarters. They arrested Boudreau for driving on a suspended license upon his arrival to ATC.

After arresting Boudreau, the Cranston Police impounded the blue Toyota Corolla in which he had returned to ATC headquarters. John Lussier also requested that the Cranston Police impound Boudreau's green Ford Explorer, which he had left parked at ATC headquarters. John Lussier explained that ATC had terminated Boudreau's employment, and that, fearing retaliation, he did not want Boudreau to have any reason to return to ATC's premises. The officers acquiesced, impounding that vehicle as well. They then conducted inventory searches of both of Boudreau's impounded vehicles, seizing various electronic devices from them.

Detective Petit then applied for and received warrants to search Boudreau's electronic devices, Yahoo! accounts, and residence. The searches that these warrants authorized yielded additional child pornography. On January 2, 2014 -- after this litigation had commenced -- Boudreau entered a plea of nolo contendere in state court to one count of possession of child pornography, and was sentenced to five years' imprisonment.

B.

Boudreau filed a pro se complaint in the District of Rhode Island on May 28, 2013, and amended it exactly three months later. His amended complaint contained five counts. Count One alleged Steven Lussier, John Lussier, and Steven Sorrel, along

with Detective Petit, illegally searched his office and office computer, and that the ATC Defendants and Cranston Defendants illegally seized and searched his two vehicles. Count Two alleged that the ATC Defendants conspired with Detective Petit to deprive Boudreau of his Fourth Amendment rights, and with Officer Carrol, Officer Bagshaw, and Sergeant Weller to entrap him into driving on a suspended license. Count Three alleged that Detective Petit made false statements in and omitted material facts from his affidavit in support of a warrant to search Boudreau's property. Count Four alleged that the ATC Defendants unlawfully intercepted his electronic communications, in violation of ECPA. Count Five alleged municipal liability against the Cities of Cranston and Warwick. Boudreau appears to have brought all of his claims against state actors (that is, everyone except for the ATC Defendants) under 42 U.S.C. § 1983.

Boudreau moved for leave to file a second amended complaint that would include a new claim under the Stored Communications Act, 18 U.S.C. § 2701, but the district court denied that motion. The parties then filed cross-motions for summary judgment on all claims. A United States Magistrate Judge issued a Report and Recommendation that the district court grant summary judgment in favor of the Cranston Defendants and Warwick Defendants on all of Boudreau's claims against them. As for the ATC Defendants, the Magistrate Judge recommended granting summary

judgment on all of Boudreau's claims against them except for his ECPA claim, for which it found summary judgment unwarranted in either party's favor. The district court, however, only adopted the Report and Recommendation in part, electing to grant summary judgment in favor of all defendants on all of Boudreau's claims. Boudreau, now represented by counsel, has appealed.

II.

We review a district court's summary judgment ruling de novo, affirming only if -- after construing the facts in the light most favorable to the non-movant and drawing all possible reasonable inferences from those facts -- no genuine material dispute of fact exists. Cooper v. D'Amore, 881 F.3d 247, 249–50 (1st Cir. 2018); Fed. R. Civ. P. 56(a). "An issue is 'genuine' when a rational factfinder could resolve it [in] either direction." Mu, 882 F.3d at 5. "A fact is 'material' when its (non)existence could change a case's outcome." Id.

On appeal, Boudreau argues that the district court erred in holding that: (1) the Cranston Defendants did not violate Boudreau's Fourth Amendment rights when they impounded and searched his two automobiles; (2) The Warwick and Cranston Defendants did not conspire to entrap Boudreau into driving on a suspended license; (3) Detective Petit did not violate Boudreau's Fourth Amendment rights upon searching his work computer; (4) Detective Petit did not violate Boudreau's Fourth Amendment rights

by making allegedly false statements in his search warrant affidavits; and (5) the ATC Defendants did not violate ECPA. We consider these arguments in turn.

A.

1.

We begin with Boudreau's arguments concerning the Cranston Defendants' impoundment and search of his two vehicles. The district court held that the "community caretaking function" justified the decision to impound those vehicles.

The "community caretaking function" is one of the various exceptions to the Fourth Amendment's requirement that law enforcement officers have probable cause and obtain a warrant before effecting a search or seizing property. United States v. Coccia, 446 F.3d 233, 237-38 (1st Cir. 2006) (citing Cady v. Dombrowski, 413 U.S. 433, 446-47 (1973)). This particular exception stems from the recognition that police officers "perform a multitude of community functions apart from investigating crime," id. at 238, including, frequently, "[d]ealing with vehicle-related problems," United States v. Rodríguez-Morales, 929 F.2d 780, 785 (1st Cir. 1991).[1] The Supreme Court has indicated

[1] The Supreme Court of Oregon has explained the justification for the exception in this way: "Our society . . . is an impersonal one. Many of us do not know the names of our next-door neighbors. Because of this, tasks that neighbors, friends or relatives may have performed in the past now fall to the police." State v.

that it is officers' non-investigatory purpose and motives when acting as "community caretakers" that justifies this exception to the warrant requirement. See Colorado v. Bertine, 479 U.S. 367, 381 (1987) ("Inventory searches are not subject to the warrant requirement because they are conducted by the government as part of a 'community caretaking' function, 'totally divorced from the detection, investigation, or acquisition of evidence relating to the violation of a criminal statute.'" (quoting Cady, 413 U.S. at 441)). And as a practical matter, imposing a warrant requirement would also likely substantially hinder officers' ability to act as community caretakers "[i]n the interests of public safety." South Dakota v. Opperman, 428 U.S. 364, 368 (1976); see also Rodríguez-Morales, 929 F.2d at 785. Therefore, when their role as "community caretakers" calls for officers to, for example, "remove vehicles that impede traffic or threaten public safety and convenience," they need not obtain a warrant before doing so. Coccia, 446 F.3d at 238.

In Coccia, the defendant argued that the community caretaking exception did not justify the officers' decision to impound his car "because the government failed to establish that the car was towed . . . pursuant to standard operating procedures." Id. We rejected that argument, explaining instead that

---

Bridewell, 759 P.2d 1054, 1068 (Or. 1988).

"impoundments of vehicles for community caretaking purposes are consonant with the Fourth Amendment so long as the impoundment decision was reasonable under the circumstances." Id. at 239; see also Rodríguez-Morales, 929 F.2d at 787 (reasoning that officers "must be free to follow 'sound police procedure,' that is, to choose freely among the available options, so long as the option chosen is within the universe of reasonable choices" (quoting Cady, 413 U.S. at 447)). It follows that, so long as the decision is reasonable, officers may impound a vehicle despite "the existence of alternative means of dealing with the automobile, even less intrusive means[.]" Rodríguez-Morales, 929 F.2d at 786. Moreover, an otherwise reasonable seizure is not rendered illegitimate "merely because it may also have been motivated by a desire to investigate crime." Coccia, 446 F.3d at 240-41.

As is usually the case, "[t]his reasonableness analysis does not hinge solely on any particular factor," but rather takes into account "all the facts and circumstances[.]" Coccia, 446 F.3d at 239 (citing United States v. Miller, 589 F.2d 1117, 1125–26 (1st Cir. 1978)). In Coccia we considered whether it was reasonable for local police officers to have towed a vehicle that was left behind after FBI agents arrested the defendant at his psychiatrist's office -- the defendant's threats during previous appointments having led his psychiatrist to contact the FBI. Id. at 236. We found that decision to have been reasonable in light

of these considerations: (1) "Coccia would be indisposed for an indeterminate, and potentially lengthy, period," and his vehicle "was filled with many of his belongings," making it "a possible target for theft or vandalism"; (2) "towing the vehicle reduced the risk of a future confrontation between Coccia and Dr. McGovern"; (3) "Coccia's comments to Dr. McGovern led to a concern that Coccia's car might contain items constituting a threat to public safety, such as explosive material, chemicals or biological agents"; (4) "there was no obvious alternative means for removing the car other than impoundment." Id. at 240; see also Rodríguez-Morales, 929 F.2d at 785-86 (holding that "under the circumstances, it was completely appropriate for the police to impound the [defendant's] car and bring it to the barracks for safekeeping" rather than leaving it abandoned on the shoulder of the highway).

Here, the Cranston Defendants' impoundment of Boudreau's vehicles was reasonable under the circumstances. First, Coccia forecloses Boudreau's argument that the Cranston Defendants' investigatory motive tainted their decision. See 446 F.3d at 240-41. Further, John Lussier's request that the Cranston Defendants remove Boudreau's cars from ATC's premises, so not to give Boudreau any reason to return, also provides strong indicia of reasonableness. Moreover, like in Coccia, Boudreau had personal possessions (including electronic devices) in his vehicles,

meaning that they otherwise could have become "a possible target for theft and vandalism." Id. at 240. Stepping back, we cannot say it was unreasonable for the Cranston Defendants to have agreed to John Lussier's request that they remove from ATC property the automobile of a recently terminated employee who had been arrested for allegedly committing crimes at work. Their impoundment of those vehicles therefore fell within the community caretaking exception and did not violate the Fourth Amendment.

The district court also held that the Cranston Defendants' subsequent inventory searches of Boudreau's impounded vehicles comported with the Fourth Amendment. It grounded that holding in our recognition in United States v. Richardson that "[t]he Fourth Amendment permits a warrantless inventory search if the search is carried out pursuant to a standardized policy." 515 F.3d 74, 85 (1st Cir. 2008) (citing Florida v. Wells, 495 U.S. 1, 3-4 (1990)). And, according to the district court, the Cranston Police Department's inventory search policy comported with Bertine's dictate that such policies may permit "the exercise of police discretion so long as that discretion is exercised according to standard criteria and on the basis of something other than suspicion of evidence of criminal activity." 479 U.S. at 375. The Cranston Police Department's inventory search policy explains that all unlocked impounded vehicles "must be inventoried . . . to protect the Department from disputes over lost or stolen property,

negligence, theft, and vandalism." Assuming favorably to Boudreau that his vehicles were in fact locked, the district court then reasoned that the same justification would nonetheless apply because the Cranston Police were also in possession of Boudreau's keys. Thus, the district court held that they exercised legitimately their discretion to inventory search his locked vehicles "on the basis of something other than suspicion of evidence of criminal activity." Id.

On appeal, Boudreau does not directly challenge the district court's determination that the Cranston Defendants properly carried out their search in conformity with the Department's inventory search policy. Rather, he tells us that this is irrelevant here, because the Cranston Defendants' investigatory motives are what actually animated their decision to conduct inventory searches. This argument, however, does not succeed. For, we have previously held that "[t]he subjective intent of the officers is not relevant so long as they conduct a search according to a standardized inventory policy." United States v. Hawkins, 279 F.3d 83, 86 (1st Cir. 2002); see also Brigham City v. Stuart, 547 U.S. 398, 404 (2006) ("An action is 'reasonable' under the Fourth Amendment, regardless of the individual officer's state of mind, 'as long as the circumstances, viewed objectively, justify [the] action.'" (quoting Scott v. United States, 436 U.S. 128, 138 (1978)); Bertine, 479 U.S. at

372, 375-76 (upholding an inventory search conducted pursuant to a standardized policy that afforded officers discretion as to whether to impound a vehicle in the absence of any showing that the police had "acted in bad faith or for the sole purpose of investigation"). And Boudreau has not argued that the officers' alleged investigatory motive was the sole motivation behind the inventory search. Accordingly, that argument is waived.

2.

We turn now to Boudreau's contention that the Cranston and Warwick Defendants -- pursuant to a conspiracy that they formed -- entrapped him into driving on a suspended driver's license. At the outset, we note that the Cranston Defendants have not taken the position that Boudreau's claim of entrapment does not allege a constitutional violation for purposes of § 1983 liability. Cf. Stokes v. Gann, 498 F.3d 483, 485 (5th Cir. 2007) (rejecting an entrapment-based § 1983 claim on the grounds that entrapment does not constitute a constitutional violation). Rather, they contend that Boudreau's claim simply fails because the facts in the summary judgment record don't add up to entrapment. Boudreau, meanwhile, anchors his entrapment claim in Detective Petit's statement to the Cranston Defendants that the ATC Defendants were "going to lure [Boudreau] back to the business and he's got a laptop in his car that I need to grab."

In the criminal context, the defense of entrapment comprises two elements: "(1) government inducement of the criminal conduct; and (2) an absence of predisposition on the part of the defendant to engage in the criminal conduct." United States v. González-Pérez, 778 F.3d 3, 11 (1st Cir. 2015). "Inducement requires not only giving the defendant the opportunity to commit the crime but also a 'plus' factor of government overreaching," such as "excessive pressure." Id. (quoting United States v. Guevara, 706 F.3d 38, 46 (1st Cir. 2013)). Moreover, "operations [that] merely give a defendant an opportunity to commit a crime, including sting operations, ordinarily do not constitute entrapment." Id. (quoting United States v. Dávila-Nieves, 670 F.3d 1, 9 (1st Cir. 2012)). Here, Boudreau, of his own volition, had been driving on a suspended license. And so we conclude that the district court did not err in granting summary judgment in favor of the Cranston Defendants on Boudreau's entrapment-related claim. As for Boudreau's allegation of a conspiracy to entrap him, that claim finds no support in the record.

3.

Next, we address Boudreau's claim that -- pursuant to a conspiracy with the ATC Defendants -- Detective Petit impermissibly searched Boudreau's office at ATC and the desktop computer located there. In rejecting this claim, the district court and Magistrate Judge both noted the Warwick Defendants'

argument that "there is no evidence that Det[ective] Petit searched Plaintiff's office." But, neither the district court nor the Magistrate Judge explicitly addressed Detective Petit's alleged search of Boudreau's office in rejecting Boudreau's Fourth Amendment claim against Detective Petit. On appeal, however, Boudreau does not direct us to any evidence in the summary judgment record that would engender a dispute of fact as to whether Detective Petit searched his office. This, therefore, does not provide grounds for overturning the district court's holding.

As for Detective Petit's search of Boudreau's computer, the district court likewise found no Fourth Amendment violation. It reasoned that "Plaintiff is correct that Det[ective] Petit could not have conducted a warrantless search of Plaintiff's office computer without his employer's permission; but here, there is uncontroverted evidence that the owner of Plaintiff's work computer gave Det[ective] Petit permission to search it." The district court cited the Ninth Circuit's decision in United States v. Ziegler as supporting the proposition that -- while Boudreau may have had a reasonable expectation of privacy in his work computer -- his employer could nonetheless provide valid consent to search the computer. 474 F.3d 1184, 1192 (9th Cir. 2007); see also United States v. Matlock, 415 U.S. 164, 171 (1974) (holding that "to justify a warrantless search by proof of voluntary consent," the government "may show that permission to search was

obtained from a third party who possessed common authority over or other sufficient relationship to the premises or effects sought to be inspected"); see also Illinois v. Rodríguez, 497 U.S. 177, 186-87 (1990) (holding that a search is not rendered unreasonable because an officer reasonably, but erroneously, believed that he had received consent from someone capable of providing it).

Boudreau argues that Ziegler's logic does not control here, because in that case the employer enjoyed "complete administrative access" to the defendant's computer, conducted "routine" monitoring of employees' computers, and provided notice to employees that their work computers "were company-owned and not to be used for activities of a personal nature." 474 F.3d at 1191-92. Boudreau presses that the summary judgment record established none of these things, and that John Lussier therefore did not have the authority to provide consent.

This fails to convince us, though, that the district court committed reversible error. We first recall that, consistent with Rodríguez, our inquiry is whether John Lussier had, to Detective Petit's mind, apparent authority to consent to the search of Boudreau's computer. See 497 U.S. at 186-87. To the extent that considerations such as those that the Ziegler court highlighted bear on whether an employer has apparent authority to consent to a search of an employee's computer, we cannot say that the law was clearly established in this respect. As a result,

even if we assume favorably to Boudreau that Detective Petit could not have reasonably believed John Lussier to be capable of consenting to the search at issue, Detective Petit would nonetheless be entitled to qualified immunity from liability on this claim. See Maldonado v. Fontánes, 568 F.3d 263, 269 (1st Cir. 2009) (citing Pearson v. Callahan, 555 U.S. 223, 230 (2009)) (setting out that in assessing whether a defendant is entitled to qualified immunity, courts "must decide: (1) whether the facts alleged or shown by the plaintiff make out a violation of a constitutional right; and (2) if so, whether the right was 'clearly established' at the time of the defendant's alleged violation"); see also Pearson, 555 U.S. at 236 (explaining that courts of appeal "should be permitted to exercise their sound discretion in deciding which of the two prongs of the qualified immunity analysis should be addressed first in light of the circumstances in the particular case at hand"). And so, we conclude that the district court did not err in granting summary judgment in favor of the Warwick Defendants on this claim. Finally, Boudreau makes no argument that, insofar as the Fourth Amendment claim against Detective Petit is resolved on qualified immunity grounds, the conspiracy claim on that issue can survive.

4.

Boudreau also presses that the district court erred in granting summary judgment of his claim that Detective Petit made

false statements in the affidavits he submitted with his application for warrants to search Boudreau's electronic devices and residence. The crux of Boudreau's argument is that Detective Petit did not mention the SSP-captured screenshots that the ATC Defendants provided him, in addition to falsely claiming that Yahoo! had not responded to a subpoena.[2]

A § 1983 plaintiff may make out a Fourth Amendment violation by showing that officers acted with at least "reckless disregard" of the "probable falsity" of their statements in support of a warrant application. Burke v. Town of Walpole, 405 F.3d 66, 81 (1st Cir. 2005) (quoting Forest v. Pawtucket Police Dep't, 377 F.3d 52, 58 (1st Cir. 2004)). So too may a Fourth Amendment violation result from officers' "intentional or reckless omission of material exculpatory facts from information presented to a magistrate." Id. However, misrepresentations or omissions of that sort only violate the Fourth Amendment when they are material to the neutral magistrate's probable cause determination. Id. at 82 (citing Franks v. Delaware, 438 U.S. 154 (1978)).

[2] Boudreau also asserts that the resulting warrants were impermissibly broad in scope. Boudreau, however, does not argue that any misdoing by Detective Petit led to the magistrate issuing an overbroad warrant. As a result, his protest that the warrant was overbroad has no bearing on his claims against Detective Petit or any of the other Defendants here.

That final requirement proves an insurmountable obstacle for Boudreau. Even if we assume that Boudreau is correct that Detective Petit intentionally or recklessly misrepresented that Yahoo! had not responded to the subpoena, and omitted that the ATC Defendants had shown him the SSP-captured screenshots, his warrant application would nonetheless have conferred probable cause. Among other things, that warrant application explained that the ATC Defendants contacted Detective Petit after discovering that Boudreau was viewing child pornography on his work computer, and that Detective Petit's "forensic preview" of that computer revealed "numerous images" of child pornography. This information is sufficient to give rise to probable cause. Therefore, even assuming favorably to Boudreau that Detective Petit's warrant affidavit included material misrepresentations and omissions, a Fourth Amendment violation cannot have resulted, because these things would not have been material to the magistrate's probable cause determination.[3]

[3] Boudreau's claim of municipal liability against the City of Cranston necessarily fails for want of a predicate constitutional violation. As for the City of Warwick -- while resolving that claim on qualified immunity grounds means that we need not reach the question of whether Detective Petit's search of Boudreau's computer violated the Fourth Amendment -- Boudreau's municipal liability claim fails because he has not met his burden of showing that the alleged constitutional violation was the result of Warwick policy or custom. See Monell v. Dept. of Soc. Servs. of City of N.Y., 436 U.S. 658, 694 (1978).

B.

We now take up Boudreau's claim that the ATC Defendants violated ECPA when, using SSP, they captured screenshots of his activity on his work computer. The district court granted summary judgment in favor of the ATC defendants on this claim, holding (1) that to make out a violation of ECPA, Boudreau needed to show a material dispute of fact that the ATC Defendants intercepted his electronic communications "contemporaneously [to their] transmission," and (2) Boudreau could not, relying only on non-expert evidence, make that showing. Boudreau asserts that the district court erred at both steps.

1.

EPCA prohibits the "intercept" of "any wire, oral, or electronic communication." 18 U.S.C. § 2511(1)(A). Interception, for purposes of the statute, is "the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device." Id. § 2510(4). An "electronic communication," in turn, is "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce." Id. § 2510(12).

"All of the circuit courts that have considered the issue" have concluded that, to constitute an "intercept" within the meaning of ECPA, "the acquisition of a communication must be contemporaneous with its transmission." Luis v. Zang, 833 F.3d 619, 628 (6th Cir. 2016) (collecting cases). Notably, however, Boudreau does not argue against the position that our sister circuits have taken. Rather, he urges us to adopt a "functional approach" to contemporaneity. Consistent with such an approach, he says, the contemporaneity requirement would be satisfied "where the defendant used technology linked to the fleeting moment in which the victim sent the electronic communication . . . even when the transmission and acquisition might have occurred moments or even hours apart." But, under this proposed approach, the contemporaneity requirement would not be satisfied when the defendant had retrieved communications from "a hard drive, server, or other permanent storage device."

In arguing for such a functional approach Boudreau relies heavily on a pair of cases from the Seventh Circuit. But, he misapprehends those cases, neither of which provide support for an approach of that sort. Boudreau tells us that in Epstein v. Epstein, the Seventh Circuit found the interception of an email to have been contemporaneous despite "a three-hour delay between when the message was sent and intercepted." See 843 F.3d 1147 (7th Cir. 2016). But that is incorrect. In Epstein, the defendant had

"surreptitiously plac[ed] an auto-forwarding 'rule' on [her husband's] email accounts that automatically forwarded the messages on his email client to her." Id. at 1148. The timestamps on the husband-plaintiff's sent emails did not match the time stamps indicating when his wife received the emails forwarded as the result of this "rule." Yet, the Seventh Circuit concluded that, at the summary judgment stage, this did not "conclusively establish" that these emails had not been intercepted contemporaneously. Id. at 1150-51. For, it held, "the interception of an email need not occur at the time the wrongdoer receives the email," but may also take place when the email is "cop[ied] at the server." Id. (emphases in original). Epstein, therefore, provides little support for the functional approach to contemporaneity that Boudreau asks us to adopt.

Boudreau also cites United States v. Szymuszkiewicz, 622 F.3d 701 (7th Cir. 2010). Similar to the facts in Epstein, the defendant in Szymuszkiewicz set up a rule in his boss's email account to forward him a copy of any email his boss received. Id. at 703. The defendant argued that he had not intercepted the emails in question because the rule merely forwarded him a copy "after the message arrive[d]." Id. (alteration in original). But the Seventh Circuit rejected that argument. It reasoned that, if the copying and forwarding occurred when the emails reached an intermediate server, then that would constitute interception. Id.

at 706. And, according to the court, it would be no different if the defendant's boss's computer "was doing the duplication and forwarding." Id. For, in that case, his boss's computer would be "effectively acting as just another router, sending packets along to their destination, and Councilman's conclusion that [ECPA] applies to messages that reside briefly in the memory of packet-switch routers" would compel the conclusion that an intercept had taken place. Id. Thus -- while suggesting that a communication may be intercepted upon its "arrival" at its intended destination -- Szymuszkiewicz does not support the functional approach that Boudreau urges us to adopt, under which we would look to whether the defendant employed "technology linked to the fleeting moment in which the victim sent the electronic communication."

Boudreau's reliance on the Sixth Circuit's decision in Luis in advocating for that "functional approach" is similarly unavailing. There, the Sixth Circuit that the plaintiff had adequately stated a claim that the defendant's use of the communications-monitoring software known as "WebWatcher" had violated ECPA. Luis, 833 F.3d at 624. In so holding, the court underscored the plaintiff's allegation that WebWatcher permits the review of the communications of another "in near real-time." Id. at 631. Any "deviation from real-time monitoring," according to the plaintiff, was not the result of "delays regarding when the

communications are acquired," but was rather attributable to "the Internet connection speed of the computer being monitored." Id. Thus, given the plaintiff's allegation that WebWatcher "records the communications as they are being sent, without regard for whether a copy is ever placed in the storage of the affected computer," the court found the plaintiff to have alleged that WebWatcher intercepted communications while they remained "in flight," and consequently, to have stated a claim that the defendant violated ECPA. Id. (quoting Szymuszkiewicz, 662 F.3d at 704). Luis, therefore, also does not support the functional approach to contemporaneity that Boudreau proposes.

In the end, that proposed approach is untenable, as it is in tension with ECPA's definition of "intercept," which includes the "acquisition of any . . . electronic . . . communication," but does not mention "electronic storage," despite the statute defining that term alongside "electronic communications." See 18 U.S.C. §§ 2510(4), (17), (12). Moreover, Congress sought to address the acquisition of no-longer-in-transit, stored communications in the Stored Communications Act. See Konop v. Hawaiian Airlines, Inc., 302 F.3d 868, 877 (9th Cir. 2002). In addition to these reasons for declining to accept what Boudreau terms the "functional approach" to contemporaneity, we also note that none of our sister circuits have adopted it. See Luis, 833 F.3d at 628; United States v. Steiger, 318 F.3d 1039, 1048-49 (11th Cir. 2003); Fraser v.

Nationwide Mut. Ins. Co., 352 F.3d 107, 113 (3d Cir. 2003); Konop, 302 F.3d at 878; Steve Jackson Games, Inc. v. U.S. Secret Serv., 36 F.3d 457, 461-62 (5th Cir. 1994).

2.

Having determined that ECPA does require that communications be intercepted contemporaneously, and rejected his functional approach to contemporaneity, we now consider whether, as Boudreau asserts, he nonetheless brought forth sufficient evidence of contemporaneity for his complaint to survive summary judgment. Boudreau leans primarily on SSP-captured screenshots depicting, among other thing, the contents of his Yahoo! Mail inbox, opened emails from others, and emails that Boudreau was in the process of drafting. It is of no consequence, says Boudreau, that he may never have sent these incomplete emails, because "[e]ven unsent Yahoo! Mail email drafts are auto-saved over the internet." Furthermore, in some of these screenshots, the web browser's "progress bar" indicates that the page displayed on Boudreau's screen was in the process of loading at the time of the screenshot. Additionally, the screenshots' timestamps match the times that Boudreau's desktop clock displays -- though the screenshot timestamps include seconds (e.g., 9:51:28), and the desktop clock shows only hours and minutes (e.g., 9:51 AM).

The district court correctly ruled that the screenshots "[do] not, on [their] face, prove contemporaneity." And it

granted summary judgment of Boudreau's ECPA claim on the grounds that expert evidence was necessary to determine whether these screenshots showed that SSP had intercepted Boudreau's communications, and that Boudreau had failed to provide evidence of that sort. On appeal, Boudreau asserts that the district court was incorrect, because lay jurors, without the aid of expert testimony, "would have been well equipped to review the key evidence in this case [and] infer that SSP intercepted electronic communication." He argues that "[s]creen-capture and webmail technology are commonplace." Thus, he says, they "fall[] within the realm of knowledge of the average lay person." See United States v. Caldwell, 586 F.3d 338, 348 (5th Cir. 2009). Thus, he says, a jury would not have needed the assistance of expert testimony to grasp these technologies' relationship to his ECPA claim.

We disagree. It may be so that a majority of individuals in the United States use and are familiar with email. And so too may a great number of people understand the concept of capturing a screenshot on an electronic device. But that isn't the inquiry here. Instead, we ask whether Boudreau could have shown that SSP contemporaneously intercepted his electronic communications relying entirely on evidence "not based on scientific, technical, or other specialized knowledge." See Fed. R. Evid. 701(c). We answer this question in the negative because apprehending whether

SSP contemporaneously intercepted his communications requires more than a lay understanding of email and the concept of capturing a screenshot. Indeed, while Boudreau insists that the screenshots in the record -- some of which depict a partially loaded "status bar" and all of which feature a timestamp showing the same number of minutes Boudreau's desktop clock -- necessarily evince contemporaneous interception, this is not so. Rather, making this determination would require an understanding of, for example, among other things, what SSP actually does (and on what sort of time-scale it does it) when it captures a screenshot, what a web browser's progress bar actually indicates, and how exactly Yahoo! Mail auto-saves emails as a user drafts them. That level of knowledge, we feel comfortable holding, is beyond that of lay jurors.[4]

This conclusion finds ample support in the body of case law that, in analyzing claims similar to Boudreau's, engages in substantial detail with the nature and workings of the technology at issue. In re Pharmatrack, Inc. Privacy Litig. -- an ECPA case in which we concluded that software designed to collect information about visitors to pharmaceutical companies' websites had

[4] Because we find the SSP-captured screenshots to have been, standing alone, categorically insufficient to show contemporaneous interception, we need not take up Boudreau's assertion that the ATC Defendants spoliated evidence by failing to preserve all of the screenshots that SSP captured.

contemporaneously intercepted the communications of those visitors -- is one such example.[5] See 329 F.3d 9, 12, 22 (1st Cir. 2003). We reached that conclusion only after considering the precise mechanism, as established though expert evidence, by which this software intercepted the communications of internet users. Id. Similarly, in Councilman, our holding that messages in "transient electronic storage" continued to constitute communications followed an extensive discussion of how exactly email client programs "us[e] packets of data to transmit information from one place to another." 418 F.3d at 69. Our sister circuits' consideration of the technology that ECPA claims implicate further reinforces the notion that more information is necessary to properly analyze Boudreau's claim here. See, e.g., Luis, 833 F.3d at 631-32; Szymuszkiewicz, 622 F.3d at 703-04; Konop, 302 F.3d at 874-75.

We, therefore, agree with the district court that for Boudreau's ECPA claim to survive summary judgment, he needed to adduce expert evidence concerning SSP's purported interception of his communications.

[5] In Pharmatrack, we found it unnecessary to determine whether ECPA requires contemporaneous interception because the evidence showed that, in any event, the communications at issue had been intercepted contemporaneously. 329 F.3d at 22.

III.

We detect no error in the district court's decision to grant summary judgment in favor of the defendants on all of Boudreau's claims. The judgment of the district court is therefore affirmed.

Affirmed.