In the

United States Court of Appeals

For the Seventh Circuit

No. 23-2905

CASSANDRA SOCHA,

Plaintiff-Appellant,

v.

CITY OF JOLIET, ILLINOIS and
EDWARD GRIZZLE,

Defendants-Appellees.

Appeal from the United States District Court for the
Northern District of Illinois, Eastern Division.
No. 1:18-cv-05681 — **Jorge L. Alonso**, *Judge*.

ARGUED APRIL 3, 2024 — DECIDED JULY 10, 2024

Before ST. EVE, KIRSCH, and LEE, *Circuit Judges*.

KIRSCH, *Circuit Judge*. Cassandra Socha, a patrol officer with the Joliet Police Department (JPD), sent a text message to her neighbor criticizing her for testifying in the criminal trial of Socha's boyfriend. Upon learning of the message, a prosecutor recommended to Sergeant Edward Grizzle that he secure a search warrant for Socha's cell phone. He did so and

thereby obtained authority to search Socha's phone for any and all data related to electronic communications.

Socha turned her phone over to Sgt. Grizzle and stressed to him that there was personal content on her phone that she wanted to remain private. To search for the text message, JPD detectives used forensic software called Cellebrite to extract all the data from her phone. They then saved the extracted data on the only computer that ran the software. Not long after the extraction, Socha heard rumors that people within the JPD had seen explicit content from her phone. Only two members of the JPD, however, admitted to seeing such content: Detectives Donald McKinney and Brad McKeon. Det. McKinney had opened a photograph on the Cellebrite computer and brought it to Det. McKeon's attention. The City asserts that Det. McKinney accessed the photograph inadvertently while opening random files in order to familiarize himself with and train on Cellebrite. Socha argues he opened her photograph intentionally and without proper authorization.

Socha sued the City of Joliet, Sgt. Grizzle, and 20 John Does. She brought multiple claims under federal and Illinois law, including, as relevant to this appeal, a claim under 42 U.S.C. § 1983 against Sgt. Grizzle for violating her Fourth Amendment rights and an intrusion upon seclusion claim under Illinois law against the City. The district court granted summary judgment to Sgt. Grizzle on the § 1983 claim and, rather than exercise its discretion to relinquish supplemental jurisdiction over the Illinois law claim under 28 U.S.C. § 1367(c)(3), also granted summary judgment to the City on the intrusion upon seclusion claim.

We agree that Sgt. Grizzle is entitled to qualified to immunity and thus conclude that the court properly granted

summary judgment in his favor on the § 1983 claim. But, as to the intrusion upon seclusion claim, we disagree with the district court and conclude that a reasonable jury could find that Det. McKinney accessed Socha's photograph intentionally and without authorization, so we reverse the grant of summary judgment on that claim.

I

Cassandra Socha has been a patrol officer with the JPD since 2014. At some point, she became romantically involved with another JPD patrol officer, Nick Crowley. In July 2017, she and Crowley had a domestic dispute at their home that resulted in Crowley being charged with reckless discharge of a firearm. Their neighbor, Maria Gatlin, provided a statement to Joliet police about the incident and later testified in Crowley's bench trial during the state's case in chief in May 2018. Crowley was acquitted of the charge.

After Gatlin's testimony and counsel's closing arguments, but before the verdict, Socha sent Gatlin a text message taking issue with her testimony. Shortly after receiving the message, Gatlin showed it to Lorinda Lamken, a Special Prosecutor with the Office of the State's Attorney's Appellate Prosecutor. Lamken believed the text message could constitute witness harassment in violation of Illinois law and, consequently, contacted Sergeant Edward Grizzle, the detective who had been assigned to investigate Crowley's criminal case. Lamken told Sgt. Grizzle that it would be necessary to secure a search warrant for Socha's phone to confirm that the message to Gatlin had come from Socha. Sgt. Grizzle then met with JPD Chief Brian Benton and Deputy Chief of Investigations Al Roechner who directed him to obtain a search warrant for Socha's phone if Lamken so desired.

After meeting with Gatlin and seeing a screenshot of the message, Sgt. Grizzle conferred with Lamken about how to draft the warrant application. Sgt. Grizzle then prepared, signed, and swore to a complaint describing his investigation and seeking a search warrant for Socha's phone. It described how Socha contacted Gatlin via text message after Gatlin testified, how Gatlin knew the message was from Socha based on the phone number, and that deleted files on a cell phone can be recovered using forensic software. He also sent the completed complaint to Lamken, who reviewed and approved it.

Sgt. Grizzle submitted the complaint to the Circuit Court of Will County, which issued a search warrant authorizing the seizure and search of Socha's phone for

> Any and all data regarding electronic communications, including dates and times of those communications, digital images or videos, e-mail, voice mail, buddy lists, chat logs, instant messaging or text accounts, forensic data as well as data pertaining to ownership and registration of the device, any and all access logs identifying who utilized said digital storage devices, and any "hidden," erased, compressed, password-protected, or encrypted files.

It also granted authority to "analyze and search any media seized for relevant evidence as outlined in this search warrant."

Later that day, Socha was brought to a conference room at the JPD station, and Sgt. Grizzle served her with the search warrant, telling her that he needed her phone. Before giving her phone to Sgt. Grizzle, Socha expressed a common concern

that there was material on her phone she did not want anyone to see. She did not describe the private material to Sgt. Grizzle.

Upon seizing the phone, Sgt. Grizzle asked Detective Christopher Botzum to extract the data from it using Cellebrite, a forensic software used to extract and analyze data from phones, including deleted files. Det. Botzum extracted the data, saved it to a folder with a non-descriptive file name that did not include Socha's name, and showed Sgt. Grizzle where it was saved. Det. German also saved the data onto a USB thumb drive and gave it to Sgt. Grizzle. Besides the thumb drive, the extracted data was only accessible on one computer in the JPD station. That computer was password protected (though the password was, simply, "Joliet"), it was in an area within the JPD investigations unit requiring keycode access, and only those who knew how to use Cellebrite could navigate the program to access the data on the computer. That said, JPD General Order 10-6 governed access to investigative files such as the phone extractions contained in Cellebrite. It set out that, "Investigative case files shall only be accessible to law enforcement personnel at the discretion of the assigned investigator or an Investigation supervisor." After finishing the extraction, the JPD returned Socha's phone to her. The data was eventually deleted from the Cellebrite computer around three weeks after it was first downloaded.

Sgt. Grizzle downloaded the extracted data onto his computer from the thumb drive, searched it by looking through pages of text messages for ones associated with Gatlin's phone number, and located the text message at issue. After Sgt. Grizzle's investigation, Socha was neither disciplined by JPD nor criminally charged in connection with the text message.

Over the summer, Socha became aware of rumors, in part via an anonymous letter, that individuals within JPD had viewed explicit content extracted from her phone. But only Detectives Donald McKinney and Brad McKeon admitted to seeing any such material. At the time, Det. McKinney, a newer detective, had been informally training on and familiarizing himself with Cellebrite at the direction of Det. German, who had given him the password to the Cellebrite computer. Defendants claim Det. McKinney, as part of the informal training, would use the Cellebrite computer to view data relevant to cases other than ones to which he was assigned. Neither Det. McKinney nor Det. McKeon were involved in investigating Socha's message to Gatlin.

At some time between the date when Socha's data was downloaded and when it was deleted, Det. McKinney accessed a media folder on Cellebrite and opened a photograph depicting a nude, female torso from the shoulders down. Det. McKinney then brought the photograph to the attention of Det. McKeon, who was sitting next to him. Det. McKeon looked at the photograph, asked Det. McKinney what the image was, and McKinney replied with something to the effect of "it might be Socha's phone" or "it could be Socha's records." Defendants contend that Det. McKinney, as part of his informal training on Cellebrite, was accessing random files to familiarize himself with the system and inadvertently opened the photograph, but Socha disputes this. They also assert that, after opening the photograph, Det. McKinney saw a thumbnail that appeared to depict a face, clicked on and viewed a second photograph in which Socha's face was visible, and then promptly closed the Cellebrite program. Socha disputes this as well.

After becoming aware of the rumors, Socha sued the City, Sgt. Grizzle, and 20 John Does raising a host of claims under federal and Illinois law. After the court granted motions to dismiss and the close of discovery, Socha's remaining claims were: (1) violation of her Fourth and Fourteenth Amendment rights under 42 U.S.C. § 1983 against Sgt. Grizzle; (2) intrusion upon seclusion under Illinois law against the City and Grizzle; and (3) invasion of privacy/publication of private facts under Illinois law against the City and Grizzle. (Socha failed to prosecute her claims against the John Doe defendants, so those were dismissed.)

Sgt. Grizzle and the City moved for summary judgment. Finding that Socha had not opposed summary judgment on the Fourteenth Amendment and invasion of privacy/publication of private facts claims, the court only addressed the merits of the Fourth Amendment claim against Sgt. Grizzle and the intrusion upon seclusion claims against the City and Grizzle. The court granted the defendants' motions, exercising (but not expressly addressing the issue of) supplemental jurisdiction over the intrusion upon seclusion claim, even though it dismissed the federal claim. Socha now appeals. She does not challenge the grant of summary judgment to Sgt. Grizzle on the intrusion upon seclusion claim, so we say no more about it.

II

We first address Socha's objection to the district court's grant of summary judgment on her § 1983 claim against Sgt. Grizzle on qualified immunity grounds. She alleges that his obtaining and executing the search warrant for her phone violated the Fourth Amendment. The district court concluded that Sgt. Grizzle was immune because Socha failed to show a

violation of clearly established law. We review a grant of summary judgment on such grounds de novo. *Kemp v. Liebel*, 877 F.3d 346, 350 (7th Cir. 2017).

Socha raises two theories on appeal to argue that the district court erred because Sgt. Grizzle violated clearly established law and is thus not entitled to qualified immunity, but neither carries the day. She asserts Sgt. Grizzle is liable because: (1) he made material omissions and misrepresentations in the warrant application; and (2) he sought, obtained, and executed an overbroad warrant.

A

A warrant request violates the Fourth Amendment if an officer, in making the request, "knowingly, intentionally, or with reckless disregard for the truth, makes false statements" that were material—that is, "necessary to the determination that a warrant should issue," *Hart v. Mannina*, 798 F.3d 578, 591 (7th Cir. 2015) (quotation omitted)—or "intentionally or recklessly with[holds] material facts," *Whitlock v. Brown*, 596 F.3d 406, 410 (7th Cir. 2010).

Proving a violation alone, however, is not sufficient for liability. Police officers sued under § 1983, like Sgt. Grizzle, are entitled to qualified immunity unless: "(1) they violated a federal statutory or constitutional right, and (2) the unlawfulness of their conduct was clearly established at the time." *Pierner-Lytge v. Hobbs*, 60 F.4th 1039, 1044 (7th Cir. 2023) (quoting *District of Columbia v. Wesby*, 583 U.S. 48, 62–63 (2018)). If either of the two prongs is not met, the officer cannot be personally liable. *Id.* We have discretion to decide which of the prongs we address first. *Id.*

We can resolve this issue under prong one: Sgt. Grizzle made no reckless, knowing, or intentional misrepresentation or omission in the warrant application. Socha contends that Sgt. Grizzle did so by misrepresenting the need to search such a broad variety of data and omitting from the application that it was possible to limit the search of her phone to only her text messages. But Sgt. Grizzle made no such misrepresentation and need not have mentioned the latter possibility. First, Sgt. Grizzle told the state court what he needed to search for (a single text message), where it could be found (the data on Socha's phone related to electronic communications), and that forensic software could be used to recover deleted data. In doing so, he gave the reasons why, at the time, he perceived the need for a broad warrant, especially because of the risk that the data had been deleted. See Wayne R. LaFave, 2 *Search & Seizure* § 4.6(d) (6th ed. 2020) ("As electronic data can be hidden in multiple formats and places in a cell phone, … it can be difficult for officers to specify in advance the sections of the device that should be searched."). There is no claim that Sgt. Grizzle lied about what he was searching for or where it might be found, and it is only "[w]ith the benefit of hindsight" that we know that his description of the places to be searched was broader than necessary. *Maryland v. Garrison*, 480 U.S. 79, 85 (1987). But "we must judge the constitutionality of [his] conduct in light of the information available to [him] at the time [he] acted." *Id.* Accordingly, expressing a need for a broad warrant was not a misrepresentation merely because, in retrospect, its breadth was unnecessary. Cf. *Edwards v. Jolliff-Blak*e, 907 F.3d 1052, 1057 (7th Cir. 2018) ("In determining whether probable cause existed, 'we look only at what the officer knew at the time he sought the warrant, not at how things turned out in hindsight.'") (quotation omitted).

Second, it is not a culpable omission to fail to state the obvious, ever-present possibility that the search could have been more limited. Warrants limit a search's scope by: (1) specifically describing the "area that can be searched"; and (2) particularly articulating the "items that can be sought" in the search. *Birchfield v. North Dakota*, 579 U.S. 438, 469 (2016). The latter is a limitation on the former. See *United States v. Mann*, 592 F.3d 779, 782 (7th Cir. 2010) ("The description of items to be seized limits the scope of the search to areas where those items are likely to be discovered."). For example, a warrant to search an RV for a handgun would necessarily permit a search to extend to more areas than would a search for a refrigerator. But, in the second situation, it cannot be a constitutional violation to omit from the warrant application that it was possible to limit the search to areas in the RV where a refrigerator might be found: that possibility is apparent because it is necessarily implied by the specific identification of the item sought. So too, here, Sgt. Grizzle identified the item he was seeking and the area he was searching; thus, he need not have stated that the search could be limited to her text messages because, in representing that he sought a text message, he made such a possibility obvious. In other words, because he specifically identified what he was looking for and where he was looking, Sgt. Grizzle made no culpable omission solely because he could have stated that it was possible to search a more limited area.

B

In raising the foregoing argument, Socha's real complaint is about the breadth of the warrant, and we share her concerns. "The Fourth Amendment requires that warrants be supported by probable cause and that they describe with

particularity the places and objects to be searched and seized." *United States v. Vizcarra-Millan*, 15 F.4th 473, 502 (7th Cir. 2021). This particularity requirement ensures that a search's scope is supported by probable cause: that each area sought to be searched is likely to yield evidence of the crime. See *id.* Another limit on the scope of a warrant is the crime under investigation, which "cabins the things being looked for" to items that could be evidence of that crime. *United States v. Bishop*, 910 F.3d 335, 337 (7th Cir. 2018). These principles apply to searches of electronic devices, including computers, *Mann*, 592 F.3d at 782, and cell phones, *Bishop*, 910 F.3d at 336–37, which are like computers in function and storage capacity, see *Riley v. California*, 573 U.S. 373, 393 (2014). Particularity is of substantial importance in the context of cell phones (and other, similar electronic devices) because, "[w]ith all they contain and all they may reveal, they hold for many Americans 'the privacies of life.'" *Id.* at 403 (quotation omitted).

Given the stakes of cell phone searches, laid bare by what happened to Socha, we remind police of their obligation to be specific and explain why there is probable cause to search every part of a cell phone they seek to search. The warrant here, based on probable cause to search for a single text message, authorized searching "[a]ny and all data regarding electronic communications, including dates and times of those communications, digital images or videos, e-mail, voice mail, buddy lists, chat logs, instant messaging or text accounts" and more. This broad language would be proper if not for the fact that officers knew exactly what evidence they were looking for and, as a matter of common knowledge, where it might be found: a single text message in her text history. Cf. *Bishop*, 910 F.3d at 336–38 (finding that a search warrant for "every file on [the defendant's] phone" was not problematically broad

because "police did not know where on his phone" the defendant kept the evidence, which included ledgers and videos).

Even if the search warrant was overbroad, though, we conclude that Grizzle is entitled to qualified immunity. Whether an officer protected by qualified immunity may be held personally liable depends on the "objective legal reasonableness" of the conduct in light of clearly established law. *Messerschmidt v. Millender*, 565 U.S. 535, 546 (2012) (quotation omitted). If an officer acted with "objective good faith" in believing the scope of a warrant was supported by probable cause, he cannot be held personally liable even if the warrant was unconstitutionally overbroad. See *id.* (quotation omitted); see also *id.* at 546 n.1 ("[T]he same standard of objective reasonableness" that applies in a suppression hearing, which includes consideration of the officer's good faith, "'defines the qualified immunity accorded an officer' who obtained or relied on an allegedly invalid warrant.") (quotation omitted).

Sgt. Grizzle—by conferring with a prosecutor before applying for the warrant and relying on the judge's issuance of the warrant—manifested an objective good faith belief that the search warrant's scope was supported by probable cause. Before drafting the application, Sgt. Grizzle sought advice from a prosecutor, Lamken, on what to include in it, and, before submitting, sent her the application for her review and approval, which she provided. That is persuasive evidence that Sgt. Grizzle held an objective good faith belief that the scope of the warrant was supported by probable cause. *Id.* at 553 (The fact that an officer "sought and obtained approval of the warrant application" from a prosecutor can support a "conclusion that an officer could reasonably have believed

that the scope of the warrant was supported by probable cause."); *Edmond v. United States*, 899 F.3d 446, 456 (7th Cir. 2018) (same). The "clearest indication" of his objective good faith is that a neutral magistrate issued the warrant. *Millender*, 565 U.S. at 546. And he can rely on that issuance to show his good faith because the warrant was not "so lacking in indicia of probable cause as to render official belief in its existence unreasonable." *Taylor v. Hughes*, 26 F.4th 419, 429 (7th Cir. 2022) (quoting *Malley v. Briggs*, 475 U.S. 335, 345 (1986)).

III

Turning to Socha's intrusion upon seclusion claim, we review a grant of summary judgment de novo, viewing the facts and drawing all reasonable inferences in favor of Socha, the non-movant. *Doe v. Gray*, 75 F.4th 710, 716 (7th Cir. 2023).

Under Illinois law, to prevail on a claim of intrusion upon seclusion, a plaintiff must show: "(1) the defendant committed an unauthorized intrusion or prying into the plaintiff's seclusion; (2) the intrusion would be highly offensive or objectionable to a reasonable person; (3) the matter intruded on was private; and (4) the intrusion caused the plaintiff anguish and suffering." *Spiegel v. McClintic*, 916 F.3d 611, 618–19 (7th Cir. 2019) (quoting *Busse v. Motorola, Inc.*, 813 N.E.2d 1013, 1017 (Ill. App. Ct. 2004)). To satisfy the first element, a plaintiff must show the defendant "intentionally intrude[d]." *Lawlor v. N. Am. Corp. of Ill.*, 983 N.E.2d 414, 424 (Ill. 2012) (quoting Restatement (Second) of Torts § 652B (1977)). Because the City argues that Det. McKinney accessed the photo while training, it effectively concedes that he was acting within the scope of his employment, so it is vicariously liable for his conduct, and Socha can raise his actions to support her claim. *Powell v. City of Chicago*, 197 N.E.3d 219, 223 (Ill. App. Ct. 2021).

The parties only dispute the first element—whether there was an unauthorized, intentional intrusion—so we express no opinion on whether the remaining elements were satisfied. Socha's claim fails if: (1) Det. McKinney was authorized to access the photograph; or (2) McKinney did not access the photograph intentionally. The district court concluded that this claim failed because Det. McKinney opened the photograph inadvertently. But Socha has presented enough evidence for a jury to reject the City's position that Det. McKinney was authorized and acted inadvertently, creating a genuine dispute of material fact that renders summary judgment on this claim inappropriate.

A

A defendant can show authorization by pointing to a state or federal statute countenancing the intrusion, see *Schmidt v. Ameritech Ill.*, 768 N.E.2d 303, 313 (Ill. App. Ct. 2002)—but the City has pointed to no statute authorizing Det. McKinney's conduct. The relationship between the intruder and the intruded-on party, such as employer-employee, can also provide authorization. See *Mucklow v. John Marshall L. Sch.*, 531 N.E.2d 941, 946 (Ill. App. Ct. 1988). In other words, the intruder can be authorized if he is acting in a "proper capacity" in committing the intrusion. *Id.* Or there can be authorization because the intruded-on party voluntarily gave up the information to the intruder, and the intruder is merely accessing its own records. See *Dwyer v. Am. Express Co.*, 652 N.E.2d 1351, 1354 (Ill. App. Ct. 1995) ("We cannot hold that a defendant has committed an unauthorized intrusion by compiling the information voluntarily given to it and then renting its compilation."). Illinois courts have also articulated a general principle, divined from the latter two bases for authorization, that

"an organization's review of its own records is not an unreasonable intrusion upon seclusion." *Schmidt*, 768 N.E.2d at 313.

The City argues that, because it, as an entity, was authorized to access Socha's data pursuant to the search warrant, so too was Det. McKinney because his intrusion, as the City's agent, was effectively just an organization reviewing its own records. But the City's position cannot be squared with its own policy. The City assumes the relevant unit of analysis for the authorization question is not the agent committing the intrusion (Det. McKinney), but the organization being sued (the City). That cannot be the case when, as here, there is an explicit policy restricting access (and thereby authorization) to certain agents within the organization. See *Zahl v. Krupa*, 850 N.E.2d 304, 312 (Ill. App. Ct. 2006) (An agent's authority arises solely from the "words and conduct of the alleged principal."). Under JPD General Order 10-6, "[i]nvestigative case files shall only be accessible to law enforcement personnel at the discretion of the assigned investigator or an investigation supervisor." The existence of this policy belies the contention that the mere securing of a warrant authorized Det. McKinney, as an agent of the City, to access Socha's data. And there is no evidence of Sgt. Grizzle, the assigned investigator, or an investigation supervisor ever giving Det. McKinney access to Socha's data such that he would be authorized under General Order 10-6.

Det. McKinney, in being permitted access to Cellebrite generally or for training specifically, could have been authorized to access Socha's data—but the record does not put this beyond dispute. There is evidence indicating that permission to access Cellebrite is sufficient to authorize access of all data therein. Det. German testified that Socha's data on Cellebrite

was located where "nonauthorized people" could not access it. This implies that those who, like Det. McKinney, were allowed to use Cellebrite were authorized to access Socha's data. The City also adduced evidence that Det. McKinney was permitted, and even encouraged, to access any and all files on Cellebrite during his training, so it could be that he was authorized to open Socha's file because he was training. But there is evidence to the contrary, demonstrating that Det. McKinney had only limited authorization to access certain files within Cellebrite that did not include Socha's. Det. Botzum attested that he had no way of securing Socha's data so "only authorized personnel" could access it, suggesting that permission to access Cellebrite is not coextensive with authorization to access all the data contained therein. Det. McKinney also remarked that he had his own file on Cellebrite containing data from cases in which he was involved. So there is a suggestion that data he was authorized to access was segregated from other data in Cellebrite and thus that he was not authorized to access data beyond his folder. Simply, the evidence points in both directions, indicating both authorization and lack thereof, creating a genuine dispute that a jury must resolve.

B

No Illinois court has expressly identified a standard for what constitutes an intentional intrusion. But given the Illinois Supreme Court's reliance on the Second Restatement of Torts in defining intrusion upon seclusion, the Restatement's definition of intent is a useful guide. It defines intent as when an "actor desires to cause consequences of his act, or that he believes that the consequences are substantially certain to result from it." Restatement (Second) of Torts § 8A (1965).

Our sister circuits, applying this definition, have concluded that an actor commits an intentional intrusion if he "believes, or is substantially certain, that he lacks the necessary legal or personal permission to commit the intrusive act." *Dubbs v. Head Start, Inc.*, 336 F.3d 1194, 1221 (10th Cir. 2003) (quoting *Fletcher v. Price Chopper Foods of Trumann, Inc.*, 220 F.3d 871, 876 (8th Cir. 2000)); *O'Donnell v. United States*, 891 F.2d 1079, 1083 (3d Cir. 1989) (same). And courts in other states that follow the Second Restatement describe intentional intrusion similarly, if not identically. *Parnoff v. Aquarion Water Co. of Conn.*, 204 A.3d 717, 732 (Conn. App. Ct. 2019); see also *Mauri v. Smith*, 929 P.2d 307, 311 (Or. 1996) ("[A]n actor commits an intentional intrusion if the actor either desires to cause an unauthorized intrusion or believes that an unauthorized intrusion is substantially certain to result from committing the invasive act in question.").

Accordingly, the question is whether Det. McKinney believed or was substantially certain that, by opening the photograph, he would be accessing Socha's data without authorization. The City argues that Det. McKinney accessed the photograph inadvertently. Its story is that Det. McKinney, as part of his informal training on Cellebrite, was indiscriminately browsing through investigative files on the Cellebrite computer to familiarize himself with the system and happened, accidentally, upon Socha's photograph.

But viewing the facts and drawing all reasonable inferences in Socha's favor, as we must, there is a genuine dispute regarding Det. McKinney's intent. While the City may ultimately prevail, that is not the question at summary judgment. Rather, we ask if there is sufficient evidence on which a reasonable jury could find for Socha. *Parker v. Brooks Life Sci., Inc.*,

39 F.4th 931, 936 (7th Cir. 2022). And a jury, faced with evidence diminishing the credibility of the City's story, could reject the City's narrative and conclude that Det. McKinney accessed Socha's photograph intentionally.

First, the location where Socha's data was saved could suggest that Det. McKinney did not act inadvertently. Det. Botzum saved Socha's extraction in a file with a name that was not identifiable with Socha, and he testified that the file was saved where "no one should be able to find [it]" and where "a normal person or a normal detective would not go." Det. McKinney may not have been a "normal detective" because he was not using Cellebrite to investigate a case; instead, he was perusing files in cases he was not assigned. But the file being saved somewhere making it difficult to locate diminishes the likelihood that Det. McKinney stumbled upon it accidentally. In other words, to a reasonable jury, Det. McKinney being able to find this hard-to-locate file suggests that he was looking for it specifically, rather than simply perusing files aimlessly.

Second, the media folders in the Cellebrite system have thumbnails previewing the contents of a file. So Det. McKinney may have seen that the media in the folder was Socha's, yet accessed the photograph anyway. Per his testimony, after he opened Socha's explicit photograph, Det. McKinney exited out from it and then clicked on the next photograph which showed her face. He noted that, before clicking on the next photograph, there was a "small thumbnail" that "looked like it had someone's face." Presumably, however, Det. McKinney could see the thumbnails before he clicked on the explicit photograph. The thumbnails might have been too small for him to identify the contents of the images precisely. But, at the

very least, it is a reasonable inference that Det. McKinney saw previews of images indicating that the file contained Socha's data and therefore intentionally opened her photograph.

Last, and most damning to the City's narrative, is Det. McKeon's testimony that, upon seeing the photograph, Det. McKinney immediately assumed it depicted Socha without any other identifying information. This statement is consistent with the foregoing evidence of the file's hard-to-find location and the thumbnails showing that the media in the folder belonged to Socha. Even taken on its own, Det. McKeon's testimony is highly indicative that Det. McKinney knew he was accessing Socha's data before he opened the photograph and thus did so intentionally.

While there are conceivable, innocent explanations for why Det. McKinney assumed the photograph might be Socha's, they are not ironclad, and a reasonable jury could reject them. First, there were rumors of explicit material on Socha's phone. But Det. McKinney did not recall when he became aware of these rumors. Thus, it is a reasonable inference that he did not know of the rumors before viewing Socha's photograph—and, if that is the case, the rumors could not explain his assumption. Second, he could have known there was an ongoing investigation of Socha involving a message from her phone, which would explain why he presumed this extracted phone data was Socha's. But Det. McKinney could not recall if he was aware of the investigation at the time he saw the photograph. And, notably, Det. McKeon was not aware of the investigation at the time, even though Sgt. Grizzle was his supervisor, suggesting not many JPD members knew of it. In sum, while the City may ultimately explain why Det. McKinney assumed the naked torso was Socha's, his assumption,

along with the evidence described above, suffices to raise a genuine dispute as to Det. McKinney's intent, rendering the grant of summary judgment improper.

C

The City urges that it is immune from Socha's intrusion upon seclusion claim under the Illinois Local Governmental and Governmental Employee Tort Immunity Act. 745 ILCS 10/2-107. It is not. The Act provides: "A local public entity is not liable for injury caused by any action of its employees that is libelous or slanderous or for the provision of information either orally, in writing, by computer or any other electronic transmission …." *Id.* We read "provision of information" to immunize conduct that involves some dissemination of information. First, the Act explains that cities are immune for providing information "orally, in writing, by computer or any other electronic transmission," so there must be some degree of communication of information. Second, it refers to "libelous or slanderous" conduct, which requires publication for liability. *Green v. Rogers*, 917 N.E.2d 450, 459 (Ill. 2009).

By its own terms, then, the Act cannot apply here: Socha's intrusion upon seclusion claim does not require her to show any "provision of information." Rather, her claim depends wholly on Det. McKinney accessing her information, not disseminating information. True, the Act has been applied to provide immunity for invasion of privacy torts. See, e.g., *Logan v. City of Evanston*, No. 20-cv-1323, 2020 WL 6020487 (N.D. Ill. Oct. 12, 2020). But courts have only applied the Act to privacy claims that require a plaintiff to show the defendant publicized, and thereby provided, information. For example, in *Ramos v. City of Peru*, 775 N.E.2d 184 (Ill. App. Ct. 2002), an Illinois court affirmed a finding that the Act rendered a city

immune to a false light invasion of privacy claim, *id.* at 188, which requires giving sufficient publicity to information, *Lovgren v. Citizens First Nat'l Bank of Princeton*, 534 N.E.2d 987, 990 (Ill. 1989) (stating the elements of false light invasion of privacy). There is no such requirement or analogous requirement for an intrusion upon seclusion claim, so the Act is inapplicable to it.

IV

Having affirmed the dismissal of Socha's § 1983 claim but rejected the dismissal of her intrusion upon seclusion claim, we briefly address the issue of supplemental jurisdiction. Socha's § 1983 claim was within the district court's original subject matter jurisdiction under 28 U.S.C. § 1331, meaning that the court could exercise supplemental jurisdiction over her intrusion upon seclusion claim under 28 U.S.C. § 1367(a). But when, as here, "federal claims drop out of the case, leaving only state-law claims, the district court has broad discretion to decide whether to keep the case or relinquish supplemental jurisdiction over the state-law claims." *Rongere v. City of Rockford*, 99 F.4th 1095, 1106 (7th Cir. 2024) (quotation omitted).

We trust the district court, on remand, to decide whether to exercise supplemental jurisdiction over Socha's intrusion upon seclusion claim. See *Williams Elecs. Games, Inc. v. Garrity*, 479 F.3d 904, 906–08 (7th Cir. 2007) (affirming a decision to relinquish supplemental jurisdiction over a state law claim remanded to the district court for a new trial after upholding the dismissal of the federal claims). In making this determination, the court "should weigh the factors of judicial economy, convenience, fairness, and comity." *Rongere*, 99 F.4th at 1106.

AFFIRMED IN PART, REVERSED IN PART, AND REMANDED