SJC-13122

COMMONWEALTH vs. AVERYK CARRASQUILLO.

Suffolk. September 8, 2021. - February 7, 2022.

Present: Budd, C.J., Gaziano, Lowy, Cypher, Kafker, Wendlandt, & Georges, JJ.

Social Media. Privacy. Constitutional Law, Search and seizure, Privacy. Search and Seizure, Expectation of privacy. Practice, Criminal, Motion to suppress.

Indictments found and returned in the Superior Court Department on July 18, 2017, and August 16, 2018.

A pretrial motion to suppress evidence was heard by Diane C. Freniere, J., and a conditional plea was accepted by Jeffrey A. Locke, J.

The Supreme Judicial Court on its own initiative transferred the case from the Appeals Court.

Suzanne Renaud for the defendant.

Ian MacLean, Assistant District Attorney (Caitlin Fitzgerald, Assistant District Attorney, also present) for the Commonwealth.

Sara E. Silva, for Massachusetts Association of Criminal Defense Lawyers, amicus curiae, submitted a brief.

GAZIANO, J. In this case we confront the novel question

whether the defendant had a constitutionally protected expectation of privacy in social media content that he shared, albeit unknowingly, with an undercover police officer.

After accepting a "friend" request from the officer, the defendant published a video recording to his social media account that featured an individual seen from the chest down holding what appeared to be a firearm. The undercover officer made his own recording of the posting, which later was used in criminal proceedings against the defendant. A Superior Court judge denied the defendant's motion to suppress the recording as the fruit of an unconstitutional search, and the defendant appealed. We transferred the matter to this court on our own motion.

Among other arguments, the defendant suggests that because his account on this particular social media platform was designated as "private," he had an objectively reasonable expectation of privacy in its contents. The Commonwealth contends that the act of posting any content to a social media account de facto eliminates any reasonable expectation of privacy in that content. Given the rapidly evolving role of social media in society, and the relative novelty of the technology at issue, we decline both the defendant's and the Commonwealth's requests that we adopt their proffered bright-line rules. Rather, as with other questions of a reasonable

expectation of privacy, each case must be resolved by carefully considering the totality of the circumstances, bearing in mind the privacy interests that the Fourth Amendment to the United States Constitution and art. 14 of the Massachusetts Declaration of Rights were designed to protect.

In the circumstances here, we conclude that the defendant did not have a reasonable expectation of privacy in the content that he shared with the undercover officer, and thus that no search in the constitutional sense occurred. Accordingly, we affirm the denial of the defendant's motion to suppress.[1]

1. Background. a. Snapchat. In order to analyze the particular circumstances in this case, where the defendant's arguments rely upon properties of the specific technology employed, some understanding of Snapchat, the social media application the defendant used to publish the video recordings at issue, is necessary. Snapchat allows users to share text, photographs, and video recordings, collectively known as "snaps." See B.L. v. Mahanoy Area Sch. Dist., 964 F.3d 170, 175 n.1 (3d Cir. 2020), aff'd, 141 S. Ct. 2038 (2021). Snaps may be shared either as "direct snaps" or as "stories." See Note, #NoFilter: A Critical Look at Physicians Sharing Patient

[1] We acknowledge the amicus brief submitted by the Massachusetts Association of Criminal Defense Lawyers in support of the defendant.

Information on Social Media, 16 Ind. Health L. Rev. 325, 329 (2019). Direct snaps are sent directly to another user's inbox, remain visible for ten seconds or less after they are opened, and can be viewed only once. See Magill, Discovering Snapchat: How Will Snapchat and Similar Self-Destructing Social Media Applications Affect Relevance and Spoliation Under the Federal Rules of Civil Procedure?, 9 Charleston L. Rev. 365, 372-373 (2015) (Magill). Stories, on the other hand, by default are shared with a larger audience, remain visible for up to twenty-four hours, and can be continuously replayed. Id. at 374. Either type of snap can be preserved if the recipient takes a screenshot[2] or otherwise records the content by some other technology external to Snapchat. Id. at 373.

Snapchat accounts can be configured as either "public" or "private." See J.E. Grenig & W.C. Gleisner, III, eDiscovery and Digital Evidence § 3:39 (Nov. 2021 update). When users initially create a Snapchat account, by default it is private, and the user must explicitly choose to make it public. See Ceres, How to Use Snapchat: Critical Tips for New Users, Wired, Oct. 2, 2018, https://www.wired.com/story/how-to-use-snapchat-filters-stories-stickers [https://perma.cc/NW6F-NKK3].

---

[2] "A 'screenshot' is a recorded image of the visible items displayed on a computer monitor [or cell phone screen]." TrueBeginnings, LLC v. Spark Network Servs., Inc., 631 F. Supp. 2d 849, 851 n.1 (N.D. Tex. 2009).

Stories posted to public accounts are visible to all members of the public, whereas stories posted to private accounts by default are visible only to individuals that the user chooses to add as "friends."[3] Id.[4] A user can add friends in one of three ways: "(1) by allowing Snapchat to access his or her phone's address book and add users who have registered using that contact information; (2) by manually inputting his or her friends' usernames; or (3) by approving other users who have requested to add the user." Magill, 9 Charleston L. Rev. at 371.

b. Factual background. We summarize the facts as found by the motion judge, "supplemented by evidence in the record that is uncontroverted and that was implicitly credited by the judge" (citation omitted). See Commonwealth v. Leslie, 477 Mass. 48,

[3] Social media "friends" are part of one another's social media network and are able to interact with each other electronically. See S.J. Drucker & G. Gumpert, Regulating Convergence 73 (2010). Friends are able to view each other's private content and directly interact via the social media application. See In re A.G., 58 Cal. App. 5th 647, 651 (2020).

[4] Even where an account is private, a user may opt to make particular stories available to the public. Hamburger, Snapchat's Next Big Thing: 'Stories' That Don't Just Disappear, The Verge, Oct. 3, 2013, https://www.theverge.com/2013/10/3/4791934/snapchats-next-big-thing-stories-that-dont-just-disappear [https://perma.cc/TVU5-5XTG]. Users also can further restrict their private stories so that the stories are visible only to specific friends. Nield, How to Control the Privacy of Your Social Media Posts, Wired, Oct. 20, 2019, https://www.wired.com/story/facebook-instagram-twitter-posts-private [https://perma.cc/93RE-W7LZ].

49 (2017), quoting Commonwealth v. Warren, 475 Mass. 530, 531 (2016). Sometime in April of 2017, Boston police Officer Joseph Connolly sent a friend request to a private[5] Snapchat account belonging to the username "Frio Fresh." Connolly sent the request from an "undercover" account that he created to aid in his investigations; the username for that account was a pseudonym chosen at "random," without regard for anyone Connolly "thought [he] might be following." The "profile picture"[6] associated with the account was a default picture assigned by

[5] Although the judge did not expressly conclude that the defendant's account was private, the evidence the judge credited established as much. "Appellate courts may supplement a judge's finding of facts if the evidence is uncontroverted and undisputed and where the judge explicitly or implicitly credited the witness's testimony." Commonwealth v. Isaiah I., 448 Mass. 334, 337 (2007), S.C., 450 Mass. 818 (2008). Here, Connolly's "uncontroverted and undisputed" testimony, which the judge explicitly credited, established that Connolly was unable to view the defendant's postings until the defendant accepted his friend request. Had the defendant's account been public, Connolly would have been able to view the content without the need for the defendant to accept a friend request. See J.E. Grenig & W.C. Gleisner, III, eDiscovery and Digital Evidence § 3:39 (Nov. 2021 update). The conclusion that the defendant's account in fact was private is not inconsistent with the judge's finding that the defendant was unaware of his privacy settings. See note 14 and part 2.c, infra.

[6] A profile picture is an image that is associated with and used to identify a particular social media user's account. See Griffith, Understanding and Authenticating Evidence from Social Networking Sites, 7 Wash. J. L. Tech. & Arts 209, 212, 217 (2012). A user's profile picture generally accompanies any content that he or she posts. See The Katiroll Co. vs. Kati Roll & Platters, Inc., U.S. Dist. Ct., No. 10-3620 (GEB) (D.N.J. Aug. 3, 2011).

Snapchat.

Once Frio Fresh accepted Connolly's friend request, Connolly was able to view stories posted to that account and would have been able to receive any direct snaps sent to him. After viewing multiple video recordings, Connolly came to believe that the Frio Fresh account belonged to the defendant. Connolly was familiar with the defendant through his work with the youth violence strike force and knew that the defendant was prohibited from carrying a firearm due to prior criminal convictions.

On May 10, 2017, Connolly viewed a story on the Frio Fresh account[7] that depicted an individual from the chest down wearing distinctive clothing and displaying what appeared to be a silver revolver. Approximately thirty minutes later, Connolly viewed another story on the account that showed the defendant inside what Connolly recognized as a weightlifting gym in the Dorchester section of Boston. Using a separate device, Connolly made a recording of the first story but was unable to record the second before it was deleted. He then notified other members of the youth violence strike force of his discovery, and officers established surveillance near the gym. Shortly thereafter, officers saw the defendant in that area, wearing the same

[7] At the evidentiary hearing, the defendant conceded that he owned the Frio Fresh account.

distinctive clothing as the individual in the Snapchat recordings. They pursued and eventually seized the defendant, recovering a revolver from his right pants pocket. The defendant was arrested and charged with multiple firearms offenses.[8]

Arguing that Connolly's actions effectuated an unconstitutional search in violation of the Fourth Amendment and art. 14, the defendant sought to suppress the video recordings and all evidence derived from them.[9] At an evidentiary hearing on the motion to suppress, both Connolly and the defendant testified. The motion judge concluded that the defendant had not established that he had had a subjective expectation of privacy in the video recordings. She also decided that, even if the defendant had had a subjective expectation of privacy in those recordings, such an expectation would not have been reasonable. Accordingly, the judge concluded that no search in the constitutional sense occurred, and denied the defendant's motion. The defendant subsequently entered into a conditional

---

[8] The defendant was indicted on charges of possession of a firearm without a license, G. L. c. 269, § 10 (a), as a subsequent offender; carrying a loaded firearm without a license, G. L. c. 269, § 10 (n); and carrying ammunition without a firearm identification card, G. L. c. 269, § 10 (h) (1).

[9] The defendant also moved to suppress the recovered revolver as the fruit of an unconstitutional seizure. This motion was denied, a decision that the defendant does not challenge on appeal.

plea arrangement, reserving his right to pursue an appeal from the denial of his motion to suppress.[10]

c. Privacy interests. The Fourth Amendment and art. 14 guarantee the right to be free from unreasonable searches. Commonwealth v. Almonor, 482 Mass. 35, 40 (2019). In interpreting these constitutional protections, we bear in mind "the circumstances under which [they were] framed, the causes leading to [their] adoption, the imperfections hoped to be remedied, and the ends designed to be accomplished." Jenkins v. Chief Justice of the Dist. Court Dep't, 416 Mass. 221, 229 (1993), quoting General Outdoor Advertising Co. v. Department of Pub. Works, 289 Mass. 149, 158 (1935). See United States v. Jones, 565 U.S. 400, 405-406 (2012) (considering historical purpose of Fourth Amendment in determining whether search occurred). As society continues to change in the face of evolving technologies, we seek to assure the same level of privacy against government intrusion that existed when the Fourth Amendment and art. 14 were adopted. See Commonwealth v. McCarthy, 484 Mass. 493, 498 (2020).

Given the substantial differences between the physical world in which our constitutions were adopted and the electronic

[10] Under the terms of the agreement, the defendant pleaded guilty to possession of a firearm without a license, as a subsequent offender, and carrying a loaded firearm without a license, and the prosecutor dismissed the remaining charge.

world that we now navigate, this task is delicate and at times fraught. See Jones, 565 U.S. at 420 (Alito, J., concurring) ("it is almost impossible to think of late-18th-century situations that are analogous to" electronic surveillance); Commonwealth v. Mora, 485 Mass. 360, 374 (2020) (same). We also are mindful that we cannot know the ways in which technology inevitably will change in years to come, and we do not wish to "embarrass the future" by adopting bright-line rules or drawing analogies that might prove ill fitting for the technology of tomorrow. See Northwest Airlines, Inc. v. Minnesota, 322 U.S. 292, 300 (1944). Therefore, in undertaking an analysis involving purported electronic searches, we avoid mechanical applications of canons designed for the physical world, and begin by returning to the founding-era principles that have informed Fourth Amendment and art. 14 jurisprudence for over two centuries. See, e.g., McCarthy, 484 Mass. at 498-500 (analyzing Fourth Amendment and art. 14 protections in light of "the underlying purposes of both art. 14 and the Fourth Amendment").

Although the word "privacy" does not appear in either the Federal Constitution or our State Constitution, the drafters of both documents undoubtedly held special regard for individual privacy. See Boyd v. United States, 116 U.S. 616, 630 (1886) (Fourth Amendment drafters sought to preserve "the privacies of life"); Commonwealth v. Blood, 400 Mass. 61, 69-70 (1987)

(drafters of art. 14 sought to protect "the right to be let alone"). Concerns over privacy, particularly privacy in communications, were "reflected in virtually every complaint levied by the colonists against King George III," and precipitated the American Revolution. See F.S. Lane, American Privacy: The 400-Year History of Our Most Contested Right 3 (2009).

The founders' deep concern for maintaining privacy against governmental intrusion eventually was enshrined in the Fourth Amendment and art. 14. See Fisher v. United States, 425 U.S. 391, 400 (1976) ("The Framers addressed the subject of personal privacy directly in the Fourth Amendment"); Commonwealth v. Sbordone, 424 Mass. 802, 810 (1997) (art. 14 was "intended to protect individual privacy interests"). Both provisions protect against governmental intrusion so that individuals may "forge the private connections and freely exchange the ideas that form the bedrock of a civil society." Mora, 485 Mass. at 371. See Berger v. New York, 388 U.S. 41, 49 (1967) (intrusions into individual privacy have been considered "subversive of all the comforts of society" since the late Eighteenth Century); Lane, supra at 16 ("the evident concern for preserving autonomy and freedom [in the Constitution] was the functional equivalent of protecting personal privacy"). To this end, the Fourth Amendment and art. 14 serve the important functions of ensuring

conversational and associational privacy.

Conversational privacy protects private conversations from unreasonable government surveillance. See United States v. United States Dist. Court for the E. Dist. of Mich., 407 U.S. 297, 313 (1972); Blood, 400 Mass. at 69 ("the right to bring thoughts and emotions forth from the self in company with others doing likewise" is protected by art. 14). Conversational privacy serves not only the Fourth Amendment's and art. 14's interests in "secur[ing] the privacies of life against arbitrary power," McCarthy, 484 Mass. at 498, quoting Almonor, 482 Mass. at 53 (Lenk, J., concurring), but also the interests protected by the First Amendment to the United States Constitution and art. 16 of the Massachusetts Declaration of rights in enabling and guarding free speech, see First Amendment (protecting "freedom of speech"); art. 16 ("The right of free speech shall not be abridged"). See Bartnicki v. Vopper, 532 U.S. 514, 533 (2001). Indeed, "[i]n a democratic society privacy of communication is essential if citizens are to think and act creatively and constructively." Id., quoting President's Commission on Law Enforcement and Administration of Justice, The Challenge of Crime in a Free Society 202 (1967) (President's Commission). The erosion of conversational privacy therefore risks imposing a "seriously inhibiting effect upon the willingness to voice critical and constructive ideas."

Bartnicki, supra, quoting President's Commission, supra.

Relatedly, associational privacy protects the ability to develop and maintain personal relationships. See Roberts v. United States Jaycees, 468 U.S. 609, 617-618 (1984) ("choices to enter into and maintain certain intimate human relationships must be secured against undue intrusion by the State"); Blood, 400 Mass. at 69 ("the right to be known to others and to know them, and thus to be whole as a free member of a free society" is protected by art. 14). Given the "vital relationship between freedom to associate and privacy in one's associations," associational privacy is necessary in order for the associations protected by the First Amendment and art. 19 of the Massachusetts Declaration of Rights to flourish. See First Amendment (protecting freedom of association); art. 19 of the Massachusetts Declaration of Rights (protecting peaceable right to assemble). See also National Ass'n for the Advancement of Colored People v. Alabama, 357 U.S. 449, 462 (1958); Society of Jesus of New England v. Commonwealth, 441 Mass. 662, 675 (2004), quoting Attorney Gen. v. Bailey, 386 Mass. 367, 380, cert. denied, 459 U.S. 970 (1982) ("The right to freedom of association [under art. 19] necessarily encompasses the right to 'privacy in one's associations' . . ."). Associational privacy "safeguards the ability independently to define one's identity" by relating to and engaging with others. Roberts, supra at 618-

619. Protection of associational privacy also plays a crucial role in maintaining a democracy; for instance, it enables individuals to amplify their voices by joining with like-minded others, and encourages civic participation by reducing isolation without fear of government interference or reprisal. See Fisher, Guilt by Expressive Association: Political Profiling, Surveillance and the Privacy of Groups, 46 Ariz. L. Rev. 621, 639 (2004). Accordingly, both the Federal and State Constitutions "must afford the formation and preservation of certain kinds of highly personal relationships a substantial measure of sanctuary from unjustified interference by the State." Roberts, supra at 618. See Blood, supra.

Government surveillance of social media, for instance, implicates conversational and associational privacy because of the increasingly important role that social media plays in human connection and interaction in the Commonwealth and around the world. For many, social media is an indispensable feature of social life through which they develop and nourish deeply personal and meaningful relationships.[11] For better or worse,

[11] See Bargh & McKenna, The Internet and Social Life, 55 Ann. Rev. Psych. 573, 581 (2004) ("on-line relationships are highly similar to those developed in person, in terms of their breadth, depth, and quality"); Bedi, Facebook and Interpersonal Privacy: Why the Third Party Doctrine Should Not Apply, 54 B.C. L. Rev. 1, 6 (2013) ("Social scientists and psychologists alike have recognized that [online] relationships can have the same

the momentous joys, profound sorrows, and minutiae of everyday life that previously would have been discussed with friends in the privacy of each others' homes now generally are shared electronically using social media connections.[12] Government surveillance of this activity therefore risks chilling the conversational and associational privacy rights that the Fourth Amendment and art. 14 seek to protect. See Jones, 565 U.S. at 416 (Sotomayor, J., concurring) ("Awareness that the government may be watching chills associational and expressive

---

qualitative structure as traditional face-to-face relationships"). See also Grimmelmann, Saving Facebook, 94 Iowa L. Rev. 1137, 1151 (2009) ("[Social media] provides users with a forum in which they can craft social identities, forge reciprocal relationships, and accumulate social capital"); Lenhart, Smith, Anderson, Duggan, & Perrin, Pew Research Center, Teens, Technology & Friendships, at 53 (Aug. 6, 2015), https://www.pewresearch.org/wp-content/uploads/sites/9/2015/08/Teens-and-Friendships-FINAL2.pdf [https://perma.cc/CWF5-HSJC] ("Given the thorough integration of social media . . . , it is no surprise that these sites play an important role in the establishment of friendships and the everyday back and forth of peer relationships").

[12] See Keller, Social Media and Interpersonal Communication, 13 Soc. Work Today, no. 3, May/June 2013, at 10 ("studies have shown that people actually are becoming more social and more interactive with others, but the style of that communication has changed so that we're not meeting face-to-face as often as we used to," but rather interacting online); Madden, Lenhart, Cortesi, Gasser, Duggan, Smith, & Beaton, Pew Research Center, Teens, Social Media, and Privacy, at 30 (May 21, 2013), https://www.pewresearch.org/internet/wp-content/uploads/sites/9/2013/05/PIP_TeensSocialMediaandPrivacy_PDF.pdf [https://perma.cc/5Z52-82ZK] ("the act of sharing certain kinds of personal information on social media profiles has become much more common" [footnote omitted]).

freedoms"); Bedi, Social Networks, Government Surveillance, and the Fourth Amendment Mosaic Theory, 94 B.U. L. Rev. 1809, 1851 (2014) ("Allowing [government monitoring of an individual] could deter an individual from exercising [his or] her rights to engage in various associational activities -- whether they are social, professional, political, or religious -- for fear the government may be watching"). Accordingly, the constitutional solicitude for conversational and associational privacy extends to the realm of social media.

2. Discussion. The defendant maintains that Connolly's conduct in viewing and recording the Snapchat stories constituted an unreasonable search in violation of the Fourth Amendment and art. 14. He argues that each of the judge's findings about his subjective expectations of privacy was error unsupported by the record, and that he did retain a subjective expectation of privacy in his Snapchat video recordings. The defendant also argues that, with respect to an objectively reasonable expectation of privacy, the court should adopt the reasoning of United States v. Chavez, 423 F. Supp. 3d 194, 203-205 (W.D.N.C. 2019), and hold that where a social media account has been set up as "private," its owner per se enjoys a reasonable expectation of privacy in content posted to that

account.[13] We review the defendant's claims under "the more stringent standards of art. 14, with the understanding that, if these standards are met, so too are those of the Fourth Amendment." Garcia v. Commonwealth, 486 Mass. 341, 349 (2020), quoting Commonwealth v. Tapia, 463 Mass. 721, 729 n.16 (2012).

a. Standard of review. "In reviewing a decision on a motion to suppress, we accept the judge's subsidiary findings of fact absent clear error but conduct an independent review of [the] ultimate findings and conclusions of law" (quotations omitted). Commonwealth v. Ramos, 470 Mass. 740, 742 (2015), quoting Commonwealth v. Colon, 449 Mass. 207, 214, cert. denied, 552 U.S. 1079 (2007). "A finding is clearly erroneous only when, although there is evidence to support it, the reviewing

[13] In the alternative, the defendant argues that even if we conclude there was no reasonable expectation of privacy, a search occurred under the trespass test. Under that test, a search occurs when "the government obtains information by physically intruding on a constitutionally protected area." Commonwealth v. Johnson, 481 Mass. 710, 715, cert. denied, 140 S. Ct. 247 (2019), quoting Grady v. North Carolina, 575 U.S. 306, 309 (2015) (per curiam). We recognize that the United States Supreme Court has held that the trespass test does not apply to "cases that do not involve physical contact, such as those that involve the transmission of electronic signals," United States v. Jones, 565 U.S. 400, 411 (2012), and accordingly consider the defendant's argument under the more protective provisions of art. 14, see Commonwealth v. One 1985 Ford Thunderbird Auto., 416 Mass. 603, 607 (1993). Even if we were to conclude that art. 14 does extend to electronic trespasses (a result we do not reach), the defendant could not satisfy the trespass test, because he consented to the officer's presence.

court on the entire evidence is left with the definite and firm conviction that a mistake has been committed" (quotations omitted). Demoulas v. Demoulas Super Mkts., Inc., 424 Mass. 501, 509 (1997), quoting Building Inspector of Lancaster v. Sanderson, 372 Mass. 157, 160 (1977). With respect to conclusions of law, "[o]ur duty is to make an independent determination of the correctness of the judge's application of constitutional principles to the facts as found." Commonwealth v. Bostock, 450 Mass. 616, 619 (2008), quoting Commonwealth v. Mercado, 422 Mass. 367, 369 (1996).

b. Whether a search occurred. To be entitled to the protections against government searches under art. 14, an individual must demonstrate that the challenged government conduct amounted to a search in the constitutional sense. Commonwealth v. Porter P., 456 Mass. 254, 259 (2010). Under the reasonable expectation of privacy test, "the government performs a search when it intrudes on a 'subjective expectation of privacy . . . that society is prepared to recognize as reasonable.'" Garcia, 486 Mass. at 350, quoting Commonwealth v. Odgren, 483 Mass. 41, 58 (2019). Thus, "a defendant must prove both a subjective and an objective expectation of privacy." Commonwealth v. Delgado-Rivera, 487 Mass. 551, 556 (2021), cert. denied, U.S. Supreme Ct., No. 21-6546 (2022).

In evaluating the existence of a subjective expectation of

privacy, a reviewing court considers "whether the individual, by his [or her] conduct, has exhibited an actual expectation of privacy." Bond v. United States, 529 U.S. 334, 338 (2000). See Mora, 485 Mass. at 366-367 (employing same standard to evaluate subjective expectation of privacy under art. 14). To have a subjective expectation of privacy, one must perceive or otherwise genuinely believe that the object of the alleged search is private. Commonwealth v. Johnson, 481 Mass. 710, 721, cert. denied, 140 S. Ct. 247 (2019). See Commonwealth v. Molina, 459 Mass. 819, 830 (2011) (Botsford, J., dissenting), citing Katz v. United States, 389 U.S. 347, 351 (1967) ("An expectation of privacy signifies a person's anticipation, belief, or understanding that he may preserve a particular place as private"). See also Black's Law Dictionary 1723 (11th ed. 2019) (defining "subjective" as "[b]ased on an individual's perceptions, feelings, or intentions"). Thus, the inquiry turns in part on what an individual knows; that is, whether the individual was subjectively aware of the presence or absence of protections in place to preserve his or her privacy. See, e.g., McCarthy, 484 Mass. at 497 n.5 (subjective expectation of privacy existed where defendant chose to "meet his codefendant in a quiet residential area"). Compare Odgren, 483 Mass. at 57-58 (no subjective expectation of privacy in telephone calls made from prison where defendant had "effective notice that his

calls . . . were subject to monitoring and recording"); Matter of a Grand Jury Subpoena, 454 Mass. 685, 688-689 (2009) (no subjective expectation of privacy in telephone calls from prison where inmates were on notice that calls were recorded).

As to whether there was an objectively reasonable expectation of privacy, "[w]hat is reasonable depends upon all of the circumstances surrounding the search or seizure and the nature of the search or seizure itself." Delgado-Rivera, 487 Mass. at 560, quoting United States v. Montoya de Hernandez, 473 U.S. 531, 537 (1985). Relevant factors in this determination include, inter alia, the precautions the individual took to protect his or her privacy; the character of the item searched; and the nature of the government intrusion. See Delgado-Rivera, supra; Commonwealth v. Krisco Corp., 421 Mass. 37, 42 (1995). While occasionally one factor may weigh so heavily that it offsets any contrary factors, ordinarily no individual factor is determinative. Porter P., 456 Mass. at 259.

c. Application. In deciding that the defendant in this case had not demonstrated a subjective expectation of privacy in his Snapchat video recordings, the judge relied upon her finding that the defendant was not "entirely aware of what his privacy settings were." At the evidentiary hearing, the defendant testified inconsistently about those settings, initially asserting that he knew his account was private, then explaining

that some of his prior stories had been posted so that everyone could see them, but that the video recordings at issue had been posted privately, and also stating that he was "not too sure" what his privacy settings were. The judge concluded that the defendant's "testimony on this point did not persuade" her, given his inconsistent statements about those settings.

In addition, notwithstanding the defendant's testimony that he would only accept as friends people that he knew, the judge observed that she could not "reconcile this testimony with that of [Connolly] who testified that he picked a user name that was not real, and that the image associated with the undercover account was a default assigned by [S]napchat"; thus, if the defendant had any policy with respect to those whom he permitted to become Snapchat friends, he did not follow his own policy in accepting Connolly's friend request. The judge also determined that the defendant did not have a reasonable expectation of privacy in the video recordings he posted on Snapchat because "[t]he nature of [S]napchat is sharing videos with other people, and even if the defendant only sent it to the people he says were following him, one hundred people by the defendant's own estimation, that was not . . . a reasonable preservation of his privacy in the video."

i. Subjective expectation of privacy. The defendant argues that, even if he was unaware of his privacy settings, we

nonetheless should infer that he had a subjective expectation of privacy by adopting the approach taken in Chavez, 423 F. Supp. 3d at 203-205. In that case, the United States District Court for the Western District of North Carolina determined that a defendant had a subjective expectation of privacy in the content of his social media because his social media account was set to be private rather than public. Id. The defendant asserts that, similarly, he enjoyed a subjective expectation of privacy in his video recordings because he maintained a private Snapchat account.

The defendant in Chavez, 423 F. Supp. 3d at 203-205, undisputedly was aware of the privacy settings applicable to his account. He stated unequivocally that his social media account was private, and also explained to the judge why he chose those particular settings. Id. at 202 ("At the hearing, Defendant testified that he implemented [restricted access to his social media content] because there was some content that he did not want 'a member of the general public . . . who was not a [social media] Friend' to see"). Although the fact that the settings were private was part of the judge's analysis, the judge did not base his conclusion solely on the account's actual privacy settings, but, rather, also relied on the defendant's awareness of those settings and the deliberate choices he made in setting them.

Here, by contrast, the judge found, and the record supports, that the defendant was unaware of his privacy settings.[14] While we at times have inferred a subjective expectation of privacy where an individual purposefully engaged in conduct aimed at ensuring privacy, see Mora, 485 Mass. at 366 (recognizing that "we have sometimes inferred an expectation of

---

[14] The defendant contends that the judge's finding that he did not demonstrate an awareness of his privacy settings was clearly erroneous and not supported by the record. We do not agree. The defendant did testify that he set up the account so that only friends could see its content. He also testified that he intentionally had posted some or all of his stories as public so that everyone could see them ("I had [my account] private, but yes, I think -- I believe I probably did at the time had it so everybody could watch my Snap"). In response to the question, "And is that the way that you had your account set up, so that everyone see your Snaps?" however, the defendant testified, "I'm not too sure. I don't remember."

Although one plausible reading of the defendant's uncertain or somewhat varying responses is that he was confused by the questions but did know that his account was private, an equally plausible reading is that he was not sure which privacy settings applied to his account. "Where there are two permissible views of the evidence, the factfinder's choice between them cannot be clearly erroneous." Commonwealth v. Carr, 458 Mass. 295, 303 (2010), quoting Demoulas v. Demoulas Super Mkts., Inc., 424 Mass. 501, 510 (1997). See Commonwealth v. Colon, 449 Mass. 207, 215, cert. denied, 552 U.S. 1079 (2007), S.C., 479 Mass. 1032 (2018) (judge's finding was not clearly erroneous where defendant's testimony was contradictory). In addition, given the irreconcilable testimony by Connolly and the defendant, which the judge emphasized, the record supports her conclusion that, if indeed he had such a policy, the defendant did not follow his asserted policy of only accepting friend requests from people that he already knew. See Commonwealth v. Yesilciman, 406 Mass. 736, 743 (1990), quoting Commonwealth v. Spagnolo, 17 Mass. App. Ct. 516, 517-518 (1984) ("a judge's resolution of . . . conflicting testimony invariably will be accepted").

privacy"); McCarthy, 484 Mass. at 497 n.5 ("We infer from the undisputed record . . . that the defendant manifested a subjective expectation of privacy in his location by choosing to meet his codefendant in a quiet residential area"), we are unable to do so where an individual was unaware of these protections. Therefore, the defendant did not satisfy his burden of demonstrating a subjective expectation of privacy.

ii. Objective expectation of privacy. To determine whether an expectation of privacy is reasonable, we consider the totality of the circumstances in the particular situation. Relevant factors in that analysis include whether the individual took ordinary precautions to protect his or her privacy, the character of the object searched, and the nature of the government intrusion. See Commonwealth v. Welch, 487 Mass. 425, 433 (2021); Commonwealth v. Berry, 420 Mass. 95, 106 n.9 (1995).

With respect to ordinary protective measures, we consider any protective measures an individual instituted to ensure that the object of the search remained within the individual's control, such that he or she could limit its exposure to others. See Delgado-Rivera, 487 Mass. at 561. In evaluating the character of the object searched, we analyze whether a defendant "controlled access to [the object] as well as whether [it] was freely accessible to others." Krisco Corp., 421 Mass. at 42. As to the nature of the government intrusion, we consider the

manner in which the government obtained the information sought to be suppressed. Almonor, 482 Mass. at 42 n.11 ("the nature of the challenged governmental conduct -- i.e., what the government does -- has always been relevant to whether such conduct implicates reasonable expectations of privacy"). Critical to this analysis is "whether the person conducting the surveillance was entitled to be where he [or she] was," Commonwealth v. Panetti, 406 Mass. 230, 232 (1989), including whether the government obtained "express or implied authorization" to be there, Almonor, supra at 43.

As the defendant points out, some protective measures were in place with respect to his Snapchat account that could support a reasonable expectation of privacy. The defendant operated a private account under a pseudonym (Frio Fresh), and friends (possible recipients) had to be added deliberately.[15] And, notably, particular features of Snapchat, including the ephemeral direct snaps and the one-day stories, preserve a certain level of privacy by design.[16] These features allowed the

[15] The defendant testified that "Frio Fresh" was a "random" name, and not a nickname by which he was known; the Commonwealth did not dispute this assertion.

[16] See Olson, Delete by Default: Why More Snapchat-Like Messaging Is on Its Way, Forbes, Nov. 22, 2013, https://www.forbes.com/sites/parmyolson/2013/11/22/delete-by-default-why-more-snapchat-like-messaging-is-on-its-way/?sh=2ca147566f31 [https://perma.cc/8DZ7-8L2U] (Snapchat is inspired by "[a]

defendant to retain a certain level of control over the content he posted, which gave rise to some level of privacy.

While the defendant's stories were less ephemeral than his direct snaps, he retained a greater level of control over them than he would have over an ordinary text message, because the stories were only temporarily available to the intended recipient and were more difficult to disburse to others. By posting the video recordings to a Snapchat story, the defendant necessarily ensured that the recordings would be deleted twenty-four hours later. See Magill, 9 Charleston L. Rev. at 374. Compare Delgado-Rivera, 487 Mass. at 561 n.7 (recognizing possibility that "ephemeral messaging" could present situation different from sending of text messages in that case). In addition, the defendant retained the ability to delete the recordings manually even before their automatic twenty-four hour expiration.[17]

Furthermore, the Snapchat stories were not as easily "disbursable by the intended recipient" as a text message. See Delgado-Rivera, 487 Mass. at 561. To disburse a Snapchat story, a recipient would have to decide to do so during the relatively

---

craving for privacy," and it is designed so that "the sender is always in control").

[17] For instance, Connolly testified that he believed the defendant deleted one of his stories shortly after posting it, thus preventing Connolly from recording the story.

brief period before the video recording was deleted, a timeline that is not applicable to those seeking to preserve a delivered text message or letter, and would have to use some external process other than Snapchat to make and store the copy before sending it onward. Thus, if a text message is akin to a letter, a Snapchat story is akin to a letter written in disappearing ink. In this way, too, the defendant retained a level of control over his stories.[18] In sum, the defendant's relative level of control over the video recordings, combined with his other protective measures, weighs in favor of his argument that he had a reasonable expectation of privacy in the posted stories.

The circumstances here thus are in contrast to the situation in Delgado-Rivera, 487 Mass. at 560, 564, where we concluded that a defendant had no reasonable expectation of privacy in his sent text messages, which police recovered from the intended recipient's device. Much like letters, those text messages became "beyond the control of the sender" once they

---

[18] Had the defendant sent the video recordings as direct snaps, as opposed to stories, he would have retained even more control over the content, because the content would have disappeared in no more than ten seconds after the recipient opened the message, thus making it even less likely that the content would be recorded or shared with others. See Magill, Discovering Snapchat: How Will Snapchat and Similar Self-Destructing Social Media Applications Affect Relevance and Spoliation Under the Federal Rules of Civil Procedure?, 9 Charleston L. Rev. 365, 372-373 (2015).

were delivered, because they were "lastingly available to" and "instantaneously disbursable by the intended recipient." Id. at 561. We reasoned that the defendant's "necessary relinquishment of control" over the messages at issue was "determinative with respect to whether [he] had a reasonable expectation of privacy in the delivered text messages." Id. at 560.

Without question, in this case the defendant's Snapchat stories were posted so as to be "[viewed] routinely by others," namely, his approximately one hundred Snapchat friends (citation omitted). See Krisco Corp., 421 Mass. at 42. Nonetheless, that the defendant electronically shared his stories with others itself is not determinative in these circumstances. Although we have held that individuals do not have a reasonable expectation of privacy in certain types of records they voluntarily conveyed to third parties, see, e.g., Smith v. Maryland, 442 U.S. 735, 742-743 (1979) (telephone call logs conveyed to telephone company); United States v. Miller, 425 U.S. 435, 444 (1976) (bank records provided to bank employees); Commonwealth v. Vinnie, 428 Mass. 161, 178, cert. denied, 525 U.S. 1007 (1998) (telephone billing records conveyed to telephone company); Commonwealth v. Cote, 407 Mass. 827, 835-836 (1990) (telephone answering service message records), we have declined to extend this reasoning to a number of broader circumstances, see

Commonwealth v. Augustine, 467 Mass. 230, 251 (2014), S.C., 470 Mass. 837 and 472 Mass. 448 (2015) (cell phone user retains reasonable expectation of privacy in cell site location information [CSLI] conveyed to cell phone companies because such information is "substantively different from the types of information and records contemplated by Smith and Miller"). Given the constitutional regard for conversational and associational privacy, the types of information and records contemplated by Smith, supra, and Miller, supra, as well as Vinnie, supra, and Cote, supra, also are categorically different from social media conversations in a constitutionally significant way.

We recognize that a majority of courts to have considered the issue of the expectation of privacy in social media content have relied exclusively upon the third-party doctrine, and have concluded that, as the Commonwealth argues, once any content is posted on social media, no reasonable expectation of privacy remains.[19] We continue to be of the view, however, that a

[19] See Palmieri v. United States, 72 F. Supp. 3d 191, 210 (D.D.C. 2014), aff'd, 896 F.3d 579 (D.C. Cir. 2018); Chaney v. Fayette County Pub. Sch. Dist., 977 F. Supp. 2d 1308, 1315-1317 (N.D. Ga. 2013); R.S. v. Minnewaska Area Sch. Dist. No. 2149, 894 F. Supp. 2d 1128, 1142 (D. Minn. 2012); United States v. Meregildo, 883 F. Supp. 2d 523, 526 (S.D.N.Y. 2012); People v. Pride, 31 Cal. App. 5th 133, 141 (2019); Everett v. State, 186 A.3d 1224, 1229 (Del. 2018), cert. denied, 139 S. Ct. 1299 (2019).

categorical rule that individuals do not maintain a reasonable expectation of privacy in information provided to third parties through electronic sources is "ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks" (citation omitted). See Augustine, 467 Mass. at 252 n.35, quoting Jones, 565 U.S. at 417 (Sotomayor, J., concurring). Compare Chavez, 423 F. Supp. at 205 ("In sum, Defendant manifested a subjective expectation of privacy in his non-public Facebook content that society is prepared to recognize as reasonable. As such, Defendant's legitimate expectation of privacy is protected by the Fourth Amendment"). Consequently, although an individual's choice to share social media content with others diminishes the individual's privacy interests, it does not per se defeat them. See Carpenter v. United States, 138 S. Ct. 2206, 2219 (2018), quoting Riley v. California, 573 U.S. 373, 392 (2014) ("the fact of 'diminished privacy interests does not mean that the Fourth Amendment falls out of the picture entirely'"). See also Commonwealth v. Feliz, 481 Mass. 689, 701 (2019), S.C., 486 Mass. 510 (2020), citing Carpenter, supra.

Nonetheless, the defendant's privacy interest in this case was substantially diminished because, despite his asserted policy of restricting such access, he did not adequately "control[] access" to his Snapchat account. See Krisco Corp.,

421 Mass. at 42. Rather, he appears to have permitted unknown individuals to gain access to his content. See id. For instance, Connolly was granted access to the defendant's content using a nondescript username that the defendant did not recognize and a default image that evidently was not Connolly's photograph. By accepting Connolly's friend request in those circumstances, the defendant demonstrated that he did not make "reasonable efforts to corroborate the claims of" those seeking access to his account. See Commonwealth v. D'Onofrio, 396 Mass. 711, 717 (1986) (no reasonable expectation of privacy in club open only to members and guests where owners did not "corroborate the claims of guest status made by persons seeking admission to the club").

Once the possibility of an undercover officer being able to view virtually all of the defendant's Snapchat content materialized, the defendant's privacy interest was further diminished. See, e.g., Commonwealth v. Price, 408 Mass. 668, 672-673 (1990) (no reasonable expectation of privacy in videotaped interaction with undercover police officer posing as drug buyer). See also Commonwealth v. DiToro, 51 Mass. App. Ct. 191, 197 (2001) (no reasonable expectation of privacy in contents of bag voluntarily displayed to undercover officer); Commonwealth v. Collado, 42 Mass. App. Ct. 464, 469 (1997), S.C., 426 Mass. 675 (1998) (no reasonable expectation of privacy

in communications with undercover officer where there was no indication that defendant and officer were "trusted friends"). Otherwise put, there is no constitutional remedy for "a wrongdoer's [mistaken] belief that a person to whom he voluntarily confides his wrongdoing" is not a government agent.[20] Hoffa v. United States, 385 U.S. 293, 302 (1966).

The nature of the government intrusion in this case further counsels against a determination that the defendant retained an objectively reasonable expectation of privacy in his video recordings, because the asserted government intrusion took place with the defendant's permission.[21] This stands in contrast to

---

[20] We do not suggest that an individual who unknowingly accepts a friend request from an undercover officer necessarily loses any reasonable expectation of privacy in the individual's Snapchat content. If, for example, a police officer had gained access to an individual's account by masquerading as a close friend or family member, the result might be different. Given the difficulty of determining an individual's true identity over the Internet, it could be that such a misrepresentation would be such that a defendant did not actually assume the risk of providing access to an undercover agent.

[21] We note that what the defendant chose to reveal by posting his stories did not include the information that Snapchat technology, like other Internet applications, includes for its own purposes in every snap or story, but that is not immediately visible to a Snapchat user. See Montie vs. Crossfire, LLC, U.S. Dist. Ct., No. 19-cv-10455 (E.D. Mich. Nov. 30, 2020). Such information, known as metadata, attaches to electronic objects such as text messages, photographs, and video recordings, and describes how, when, and by whom the item "was collected, created, accessed, or modified and how it is formatted." Williams v. Sprint/United Mgt. Co., 230 F.R.D. 640, 646 (D. Kan. 2005). For example, the metadata that attaches to

our conclusion that "pinging"[22] a cell phone violated a reasonable expectation of privacy in part because pings are "initiated and effectively controlled by the police . . . without any express or implied authorization or other involvement by the individual cell phone user." Almonor, 482 Mass. at 43. See Carpenter, 138 S. Ct. at 2220 (reasonable expectation of privacy in CSLI because "a cell phone logs a cell-site record by dint of its operation, without any affirmative act on the part of the user beyond powering up"); Augustine, 467 Mass. at 249-251, 255 (reasonable expectation of

---

Snapchat content can reveal the sender's location, device address, and mobile telephone number. See Bungert, Do It for the Snap: Different Methods of Authenticating Snapchat Evidence for Criminal Prosecutions, 2021 U. Ill. J.L. Tech. & Pol'y 121, 135 (2021); Levinson-Waldman, Government Access to and Manipulation of Social Media: Legal and Policy Challenges, 61 Howard L.J. 523, 554 n.166 (2018). While invisible within Snapchat, metadata can be extracted from Snapchat content using other applications. Helget v. Hays, 300 F.R.D. 496, 500 (D. Kan. 2014). Although such information is not at issue here, we recognize the difference between information that is purposefully revealed by the user of an electronic device and that unknown information that is created or shared through technological processes absent any input by the user, the latter of which we have excluded from the analysis of a decision to share information with a third party. See Commonwealth v. Augustine, 467 Mass. 230, 251 (2014), S.C., 470 Mass. 837 (2015).

[22] "Pinging" is the process of causing a cell phone to "transmit its global positioning system (GPS) coordinates to the [cellular service] provider," which then can be provided to police to assist in locating the individual in possession of that device. Commonwealth v. Almonor, 482 Mass. 35, 36 & n.1 (2019).

privacy in CSLI because CSLI is "purely a function and product of cellular telephone technology" that is conveyed to cellular service provider without any action or consent by user).

Here, the challenged recordings "effectively [had been] controlled by [the defendant]" and were made accessible to the undercover officer only with the defendant's "express or implied authorization." Almonor, 482 Mass. at 43. Indeed, Connolly was able to view the defendant's stories precisely because the defendant gave him the necessary permissions to do so. That the defendant not only did not exercise control to exclude a user whose name he did not recognize, but also affirmatively gave Connolly the required permissions to view posted content, weighs against a conclusion that the defendant retained a reasonable expectation of privacy in his Snapchat stories.

The defendant maintains that his "permission" should not be considered valid, given that it was obtained via a ruse. That Connolly did not reveal his true identity to the defendant, however, does not vitiate the permission the defendant extended to him. See Hoffa, 385 U.S. at 300, 303 (rejecting argument that informant's "failure to disclose his role as a government informer vitiated the consent that the [defendant] gave to [him]"); Commonwealth v. Sepulveda, 406 Mass. 180, 182 (1989) ("It makes no difference that the defendant's consent to police entry was obtained by a ruse"). See also 4 W.R. LaFave, Search

and Seizure § 8.2(m) (6th ed. 2021) ("consent is not vitiated merely because it would not have been given but for the nondisclosure . . . of the other person's identity as a police officer or police agent"). Indeed, to hold otherwise would require police officers to "identify themselves as [such] when they investigate criminal activity," thus rendering "virtually all undercover work" unconstitutional. United States v. Butler, 405 Fed. Appx. 652, 656 (3d Cir. 2010). This we decline to do. See Commonwealth v. Garcia, 421 Mass. 686, 692 (1996) ("undercover police work is a legitimate investigative technique").

Order denying motion to suppress affirmed.