COMMONWEALTH OF MASSACHUSETTS

Supreme Judicial Court

No. SJC-13122

COMMONWEALTH,
APPELLEE,

v.

AVERYK CARRASQUILLO,
APPELLANT.

ON THE DEFENDANT'S APPEAL FROM AN ORDER OF THE SUFFOLK SUPERIOR COURT DENYING HIS MOTION TO SUPPRESS

BRIEF OF AMICUS CURIAE MASSACHUSETTS ASSOCIATION OF CRIMINAL DEFENSE LAWYERS

Sara E. Silva (BBO #645293)
Hogan Lovells US, LLP
125 High Street, Suite 2010
Boston, MA 02110
(617) 371-1000
sara.silva@hoganlovells.com

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page

CASES

STATUTES

RULES

OTHER AUTHORITIES

CORPORATE DISCLOSURE STATEMENT

Pursuant to Supreme Judicial Court Rule 1:21, the Massachusetts Association of Criminal Defense Lawyers ("MACDL") states it is a 501(c)(6) corporation organized under the laws of the Commonwealth of Massachusetts. MACDL does not issue stock or have parent corporations, and no publicly held corporations own stock in MACDL.

PREPARATION OF AMICUS BRIEF

Pursuant to Mass. R. App. P. 17(c)(5), MACDL and its counsel declare that:

(a) no party or party's counsel authored this brief in whole or in part;

(b) no party or party's counsel contributed money to fund preparing or submitting this brief;

(c) no person or entity, including amicus curiae, contributed money that was intended to fund preparing or submitting this brief; and

(d) counsel has not represented any party in this case or in proceedings involving similar issues, or any party in a case or legal transaction at issue in the present appeal.

INTEREST OF AMICUS CURIAE

MACDL represents more than 1,000 trial and appellate lawyers who are members of the Massachusetts Bar and devote a substantial part of their practices to criminal defense. MACDL files amicus briefs in cases raising questions important

to the criminal justice system. See, e.g., *Commonwealth v. Delgado-Rivera*, 487 Mass. 551 (2021).

INTRODUCTION & SUMMARY OF ARGUMENT

The Boston Police Department has created and used an unknown number of accounts on Snapchat, a social media platform, to lure users into accepting their "friend" requests, so that the police can electronically surveil and record private communications sent by those users to their Snapchat friends. The police have done so with no judicial oversight; no probable (or frankly any) cause; and no constraints on what they will surveil or record, or how long their surveillance will last.

The Commonwealth urges this Court to approve this practice and affirm the trial court's conclusion that even if a person has a subjective expectation of privacy in communications shared within their circle of Snapchat friends, "that expectation is not one that society objectively recognizes as reasonable." See R.A.36. Its argument rests upon a single premise: if a person is friends with "over one hundred people" on social media, then that person cannot expect privacy in the communications sent to those friends, and any information so shared is inherently "public" information. See Appellee's Br. at 7.

This Court should reverse. As more fully set forth below, neither this Court nor the Supreme Court has ever equated privacy with secrecy. Information does not become public to the world as a matter of law just because someone shares it with

friends, even if the person has lots of friends and even if they communicate online instead of in person. As this Court recognized just last year, Article 14 of the Declaration of Rights and the Fourth Amendment to the U.S. Constitution were designed to "preserve the people's security to forge the private connections and freely exchange the ideas that form the bedrock of a civil society." *Commonwealth v. Mora*, 485 Mass. 360, 371 (2020). Secretly monitoring in real time every communication the defendant sent within his private network for a 30-day period violated the defendant's right to commit his private thoughts "only to the sight of his friends." Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 Harv. L. Rev. 193, 198 n.2 (1890) (internal citation omitted). That is an expectation of privacy that our society has long held to be not only reasonable, but fundamental.

But this undercover activity is even more sinister because unbounded government surveillance of private communications reaches far beyond the rights of the surveilled -- it shakes the foundational concepts *Mora* recognized as forming the bedrock of our society. Indeed, the police practice at issue in this case threatens basic concepts of individual freedom:

> [T]raditional authoritarian societies create procedures to watch and listen secretly to elite groups, and modern totalitarian governments keep extensive records on individuals, families, and all associational activities. In contrast, . . . constitutional governments are expressly barred by bills of rights and other guarantees of civil liberty from interfering with the citizen's private beliefs, associations, and acts, except in extraordinary situations and then only through controlled procedures.

Stephen E. Henderson, *Expectations of Privacy in Social Media*, 31 Miss. C. L. Rev. 227, 230 & n.9 (2012) (*quoting* Alan F. Westin, *Historical Perspectives on Privacy: From the Hebrews and Greeks to the American Republic* 4-5 (unpublished manuscript, distributed in 2009));[1] accord *Mora*, 485 Mass. at 372 (citation omitted).

Article 14 and the Fourth Amendment preclude the police from unilaterally listening in on private telephone calls, sticking electronic devices on walls or in cars, or generally using new technology to learn what would otherwise be unknowable without the investment of substantial investigative resources.[2] In addition, Articles 1, 10, and 16, and the First, Fifth, and Fourteenth Amendments, protect our fundamental rights as citizens of a free democracy to freely associate and speak together, and enjoy due process and the equal protection of our laws -- rights that are severely threatened by the police action in this case.

---

[1] China, for example, has begun using digital surveillance of social media to quash political dissent in Hong Kong. See, e.g., Vivian Wang & Alexandra Stevenson, *In Hong Kong, Arrests and Fear Mark First Day of New Security Law*, N.Y. Times (updated July 13, 2020), available at https://www.nytimes.com/2020/07/01/world/asia/hong-kong-security-law-china.html.

[2] See *Mora*, 485 Mass. at 375-376; see generally, *Commonwealth v. Almonor*, 482 Mass. 35 (2019); *Commonwealth v. Johnson*, 481 Mass. 710 (2019); *Commonwealth v. Fulgiam*, 477 Mass. 20 (2017); *Commonwealth v. Rousseau*, 465 Mass. 372 (2013); *Commonwealth v. Blood*, 400 Mass. 61 (1987); see also *Carpenter v. United States*, 138 S. Ct. 2206 (2018); *Riley v. California*, 573 U.S. 373 (2014); *Jones v. United States*, 565 U.S. 400 (2012); *United States v. U.S. Dist. Ct. for E. Dist. of Mich., S. Div.*, 407 U.S. 297 (1972); *Katz v. United States*, 389 U.S. 347 (1967).

Social media may be an evolving technological medium, but it furthers a treasured form of communication this Court has long protected -- the sharing of private thoughts and experiences among friends. The features that render social media a potent communication tool by making it easier for people to meet, associate, and share their thoughts do not preclude constitutional privacy protections. To the contrary, where a social media platform itself distinguishes between "public" and "private" communications, as Snapchat does, and where a user communicates within the designated "private" sphere, as this defendant did, that should be sufficient to invoke constitutional protections.

The Commonwealth would require social media users to ignore actual distinctions between "public" and "private" communications, and instead assume the risk of warrantless police surveillance. But "assumption of the risk" principles do not (and should not) permit the police conduct at issue here. This Court should reject the Commonwealth's proposal in favor of a straightforward rule recognizing that users expect privacy when communicating via "private" channels on social media platforms. As more communication migrates to the Internet, smartphones, and social media, constitutional protections must move with them, and those protections preclude police from surveilling or recording private communications without probable cause to suspect criminal activity and a judicial warrant.

STATEMENT OF THE CASE AND FACTS

On May 10, 2017, Boston police officers arrested the defendant for unlawfully possessing a firearm. R.A.21. The information used to identify, locate, and stop the defendant was based solely on information gleaned from the defendant's private Snapchat account, which police had been surveilling for one month without a warrant or any quantum of individualized suspicion. See R.A.32-33; Tr.31:10-11.

A. Relevant Features of Snapchat

Snapchat is a social media application that allows account holders to post information to the public at large and/or send information to a selected group of "friends" or "followers." Opening an account on Snapchat requires only that a person download the application; provide their first and last name, a telephone number or email address, and a birthdate; and select a username and password that is not already in use on Snapchat. See Snapchat Support: Create a Snapchat Account, available at https://support.snapchat.com/en-US/a/account-setup. By default, Snapchat profiles are private; however, if a Snapchat user is 18 or older, they can opt to create a "Public Profile," which allows them to share "with a wider audience (beyond their immediate friends)." See Public Profile and Creator Account FAQ, available at https://support.snapchat.com/en-US/a/creator-faqs. However, Snapchat is "primarily designed for visual communication with close friends." *Id.*

To communicate privately, Snapchat users send requests to other users asking to "friend" or "follow" them; such requests are received by the other user via an electronic message, which the recipient can then accept, reject, or ignore. See Add Friends, available at https://support.snapchat.com/en-US/a/add-friends. If a request is accepted, the sender of the request will thereafter receive information sent out by their new "friend;" these communications are referred to as "Snaps" and "Chats." See Snaps & Chats, available at https://snap.com/en-US/privacy/privacy-by-product. Snapchat communications are typically visual as opposed to verbal; they primarily consist of photographs, short (10 second) videos, emojis, or other forms of visual communication. See Create a Snap, available at https://support.snapchat.com/en-US/a/capture-a-snap. Each individual Snapchat user can choose whether to post communications publicly or send them privately to their friend list. See Snaps & Chats, https://snap.com/en-US/privacy/privacy-by-product.

Snapchat intends Snaps and Chats to be "[j]ust like talking to someone in person or on the phone," and tells users they can "express whatever's on your mind at the time -- without automatically keeping a permanent record of everything you've ever said." *Id*. This is because Snapchat messages are ephemeral -- or, as Snapchat puts it, "Deletion is our default." Our Privacy Principles, available at https://www.snap.com/en-US/privacy/privacy-center; see also When Does Snapchat

Delete Snaps and Chats, available at https://support.snapchat.com/en-US/a/when-are-snaps-chats-deleted. Snapchat servers are designed to automatically delete Snaps sent to a friend group as soon as they have been viewed by all recipients or after a set period, whichever is earlier.[3] See *id.* A recipient can replay a Snap only if they are in the Friends screen on Snapchat and the Snap has not yet been deleted; as soon as the recipient exits the Friends screen, they can no longer replay a Snap. See View a Snap, available at https://support.snapchat.com/en-US/a/view-snaps.

Snaps can be saved by a recipient, but only with notice to the sender. See Snaps & Chats ("Saving Snaps was designed with privacy in mind. You control whether your Snaps can be saved."), https://snap.com/en-US/privacy/privacy-by-product. If a Snap is saved in the application itself, the sender can unilaterally delete it, and Snapchat will then remove the Snap from the application, remove the Snap from its own servers, and attempt to remove the Snap from all of the sender's friends' devices. See When Does Snapchat Delete Snaps and Chats, https://support.snapchat.com/en-US/a/when-are-snaps-chats-deleted. A recipient can also "record" a Snap while they are watching it by using a smartphone to take a screenshot or video of a Snap while it is being viewed. See Snaps & Chats, https://snap.com/en-US/privacy/privacy-by-product. If a recipient does so,

[3] In 2017, messages were removed after 24 hours See Tr.14:13-16, 34:4-7.

however, Snapchat alerts the sender immediately.[4] In this case, the police appear to have precluded Snapchat from sending an alert to the defendant by viewing the defendant's Snap on one device while using a second device to record it. See Tr.23:3-8.

B. The Boston Police Department's Snapchat Surveillance

During the evidentiary hearing on the defendant's motion to suppress, the officer acknowledged that he has friended an undisclosed number of individuals on Snapchat using the same username that he used with the defendant. See Tr.29:17-19, 30:6-9, 33:1-4, 35:4-5. Other Boston police officers also use Snapchat as a part of their police work, despite the fact that none have been trained on how to use it. See Tr.30:10-15, 41:6-9; see also *Commonwealth v. Dilworth*, 485 Mass. 1001, 1003 n.4 (2020) (referencing 22 other pending cases involving charges stemming from Snapchat surveillance). There appear to be no policies or even supervision governing these warrantless, suspicionless electronic surveillance efforts by police.

Before gaining access to the defendant's "Frio Fresh" private Snapchat account, the police officer did not even know that the account belonged to the defendant. After gaining access to the account -- using what the court assumed was

[4] See Steven John, *'Does Snapchat Notify Users When You Yake Screenshots?': Here's What You Need to Know*, Business Insider (Oct. 28, 2019), available at https://www.businessinsider.com/does-snapchat-notify-screenshots#:~:text=Snapchat%20does%20notify%20people%20when,section%20of%20a%20user%27s%20story.

a fake name intended to "resonate with the audience he was attempting to try to . . . snoop on," Tr.74:16-24 -- the officer was able to use the content of the defendant's private Snaps, which included an undisclosed number of videos and photographs, to identify the defendant as the account owner. See R.A.32. For one month, the officer reviewed the content of every communication sent by the defendant to his private friend network without any judicial supervision and without any limitation on the scope or length of the surveillance or which communications he could record. See Tr.31:10-11.

ARGUMENT

I. Individuals Have a Reasonable Expectation of Privacy in Communications Sent to Their Friends Via "Private" Communication Channels Provided by Social Media Platforms Like Snapchat.

A. Individuals Have a Constitutionally Protected Right to Conversational Privacy.

Conversational privacy -- that is, the right to share information with others without law enforcement listening in -- is one of the oldest rights protected by Article 14. See, e.g., *Blood*, 400 Mass. at 71-72, 74. Article 14 was:

> intended by its drafters not merely to protect the citizen against the breaking of his doors, and the rummaging of his drawers, but also to protect Americans in their beliefs, their thoughts, their emotions and their sensations by conferring as against the government the right to be let alone -- the most comprehensive of rights and the right most valued by civilized men.

Id. at 69 (quotations and internal punctuation omitted). This Court has squarely held that the right to be let alone includes conversational privacy -- that is, "the right to

bring thoughts and emotions forth from the self in company with others doing likewise" without being subjected to warrantless, suspicionless government surveillance. *Id.*

As with Article 14, the "basic purpose" of the Fourth Amendment "is to safeguard the privacy and security of individuals against arbitrary invasions by governmental officials." *Carpenter*, 138 S. Ct. at 2213 (quoting *Camara v. Municipal Court of City and Cnty. of San Francisco*, 387 U.S. 523, 528 (1967)). The Amendment was our nation's "response to the reviled 'general warrants' and 'writs of assistance' of the colonial era, which allowed British officers to rummage through homes in an unrestrained search for evidence of criminal activity," and a "central aim" of the Fourth Amendment was "to place obstacles in the way of a too permeating police surveillance." *Id.* at 2213-14 (*quoting Riley*, 573 U.S. at 403; *United States v. Di Re*, 332 U.S. 581, 595 (1948)).

Just as "society's expectation has been that law enforcement agents and others would not -- and indeed, in the main, simply could not – secretly monitor and catalogue every single movement of an individual's car for a very long period," *id.* at 2217 (quoting *Jones*, 565 U.S. at 430), society expects that law enforcement agents will not (and cannot) monitor, catalogue, and record the content of our private communications. See, e.g., *Katz*, 389 U.S. at 352. Indeed, our society is built on the concept that we can communicate with each other without fear of "tireless and

absolute surveillance." *Carpenter*, 138 S. Ct. at 2218. Even people who communicate privately from locations in which they might not otherwise have a reasonable expectation of privacy (e.g., a business office, a friend's apartment, a taxicab, or a public phone booth) "may rely upon the protection of the Fourth Amendment" to preclude the government from monitoring or recording those communications absent probable cause and a warrant. *Katz*, 389 U.S. at 352. Simply put, Article 14 and the Fourth Amendment protect against official intrusion into private communications, regardless of where or how those communications take place.

B. Users Reasonably Expect Privacy When They Use Private Communication Channels Provided by Social Media Applications Like Snapchat.

The Supreme Court has repeatedly warned courts to pay "attention to Founding-era understandings . . . when applying the Fourth Amendment to innovations in surveillance tools." *Carpenter*, 138 S. Ct. at 2214. In *Carpenter*, the Supreme Court acknowledged that individuals have no right to privacy in the voluntary movements of a vehicle on public streets when tracked in a "limited" fashion during a "discrete" trip, but held that different constitutional principles apply to cell-site location information, because that type of information more closely resembles 24-hour surveillance. *Id.* at 2215.

The same conclusion applies here. Our founders abhorred warrantless governmental surveillance of our private conversations. That principle has guided decades of constitutional analysis, and the law has attempted to keep pace with technological advances irrespective of whether the conversations take place in person, on the telephone, or, as here, through a social media platform.

Social media has become a primary mode of communication in this country. As of 2017, seven out of ten American adults used at least one social media platform, with Facebook alone having 1.79 billion active users, a number that represents "about three times the population of North America." *Packingham v. North Carolina*, 137 S. Ct. 1730, 1735 (2017). Snapchat currently has 500 million monthly active users, nearly 2/3 more than the population of the United States. See Salvador Rodriguez, *Snap Reaches 500 Million Monthly Users*, NBC (updated May 20, 2021), available at https://www.cnbc.com/2021/05/20/snap-reaches-500-million-monthly-users.html. Three out of four adults between the ages of 18 and 24 who were surveyed on their social media use reported using Snapchat, and 71% of users between the ages of 18 to 29 reporting using Snapchat at least once per day. Brooke Auxier & Monica Anderson, *Social Media Use in 2021*, Pew Rsch. Ctr. 5, 8 (Apr. 7, 2021), available at https://www.pewresearch.org/internet/2021/04/07/social-media-use-in-2021/. In short, social media has become "such a pervasive and insistent part of daily life" that, for most people, using it has become indispensable to participation

in modern society. Accord *Carpenter*, 138 S. Ct. at 2220 (quoting *Riley*, 573 U.S. at 385). Like the public telephone discussed in *Katz* and the personal cell phones discussed in *Riley* and *Carpenter*, social media platforms have created a "seismic shift" in the manner in which we communicate with each other. *Packingham*, 137 S. Ct. at 1735-1736.

The breadth of communications made possible by social media touch on all manner of personal or highly confidential information, particularly in contexts where privacy protections exist. Most social media sites permit users to choose between public and private postings. Public postings consist of "all content visible to any person who views the user's account on a social media platform without being explicitly granted permission to do so (in other words, not a 'friend' or 'connection' of the user . . .)." Nicole A. Keefe, *Dance Like No One Is Watching, Post Like Everyone Is: The Accessibility of 'Private' Social Media Content in Civil Litigation*, 19 Vand. J. Ent. & Tech. L. 1027, 1030-1031 (2017); accord Black's Law Dictionary (11th ed. 2019) (defining "public" as "[o]pen or available for all to use, share, or enjoy"). Private postings, in contrast, are those in which users provide viewing access only "to a specific group of people . . . typically referred to as the user's 'friends,' 'followers,' or 'connections,' depending on the platform." Keefe, 19 Vand. J. Ent. & Tech. L. at 1031. Some platforms, like Snapchat, add onto this privacy protection by rendering a user's communications ephemeral, meaning they

automatically disappear within a set period of time; Snapchat expressly encourages its users to expect their communications will function like an oral conversation. See Our Privacy Principles, available at https://www.snap.com/en-US/privacy/privacy-center ("Snapchat aims to capture the feeling of hanging out with friends in person -- that's why Snaps and Chats are deleted from our servers once they're opened or expired.").

To be clear, this case does not present the question of whether there is a reasonable expectation of privacy in social media postings that can be seen by anyone, or are posted in areas specifically designated as "public" within the social media platform.[5] The issue presented by this case is the easier question of whether law enforcement can trick their way into an area from which they can monitor and record the content of private communications sent via Snapchat for as long as they want without any temporal or content-based limitations, individualized suspicion, or oversight of any kind.

[5] The use of technology to conduct intrusive, effortless, and comprehensive surveillance of a person's activity, even in a genuinely public space, can still constitute a search. See *Polay v. McMahon*, 468 Mass. 379, 384 (2014); accord *Carpenter*, 138 S. Ct. at 2217; *Jones*, 565 U.S. at 430 (Alito, J., concurring in judgment); *Mora*, 485 Mass. at 376. Although long-term surveillance and aggregation of an individual's social media comments could conceivably violate privacy rights under certain circumstances, that issue is not currently before the Court.

The answer to that question must be no. When users limit their communications to a specific group of people, as was done in this case, they have literally availed themselves of the right to commit their private thoughts "only to the sight of [their] friends." Warren & Brandeis, 4 Harv. L. Rev. at 198 n.2 (internal citation omitted). Sharing information with one's friends, no matter how many or how few, falls well within the right to conversational privacy. "Privacy is not a discrete commodity, possessed absolutely or not at all." *Smith v. Maryland*, 442 U.S. 735, 749 (1979) (Marshall, J., dissenting). An individual might have a marginally reduced privacy interest in information shared with others, but "diminished privacy interests does not mean that the Fourth Amendment falls out of the picture entirely." *Riley*, 573 U.S. at 392. Or, as one federal court recently put it, "your sensitive information does not lose the label 'private' simply because your friends know about it. Your privacy interest in that information may diminish because you've shared it with your friends, but it does not necessarily disappear." *In re Facebook, Inc. Consumer Privacy User Profile Litig.*, 402 F. Supp. 3d 767, 796 (N.D. Cal. 2019).

The police conduct at issue in this case is substantially more intrusive and revealing than in other contexts already deemed constitutional searches. See *Carpenter*, 138 S. Ct. at 2219 (cell-site location information); *Jones*, 565 U.S. at 404 (GPS monitoring); *Mora*, 485 Mass. at 375 (pole cameras); *Almonor*, 482 Mass. at

47-48 (cell-phone "ping"). Those cases were largely animated by concern that the government could use electronic surveillance of a person's movements to inferentially reveal one's activities and associations. Here, the police surveilled private information directly by tricking their way into the defendant's friend group and thereafter monitoring and recording what he said. Affirming that conduct would lead to the bizarre result that law enforcement could not unilaterally monitor our movements on public streets for 28 days, but would be free to monitor and record our private communications for 30 days or longer. Compare *Jones*, 565 U.S. at 403-404 (unconstitutional to use GPS to track car for 28 days) with Tr.31:10-11 (police monitored defendant's Snapchat communications for one month).

The Commonwealth's brief repeatedly sidesteps the intrusiveness of the police surveillance in this case by characterizing the communications at issue as "public" instead of private. See, e.g., Appellee's Br. at 7 ("the defendant lacked a reasonable expectation of privacy in information that he publicly posted"); see also *id.* at 14-16, 23. But calling the defendant's communications "public" does not make them so. As described *supra*, Snapchat users can choose between public posts that can be viewed by everyone on Snapchat, and private messages that are sent only to a user's selected friend list. There is no dispute that, in this case, the police could not view the defendant's messages until they were able to join his friend list.

Tr.15:19-16:3.[6] The communications at issue here were not "public" as that term is used on Snapchat, or as it is commonly understood in general parlance; a wedding is not a "public" event just because 100 people attend it.

The Commonwealth's argument rests on a single unsubstantiated premise -- that speaking to 100 Snapchat friends is the legal equivalent of speaking to the public at large. But placing the numbers of friends in context easily proves the logical flaw in that reasoning. When a Snapchat user chooses to post publicly, the potential listening audience consists of 500 million other active users. Those mind-bogglingly large numbers are part of what makes social media so potent. See, e.g., *Packingham*, 137 S. Ct. at 1735-1736. The defendant here did not send messages to 500 million people; instead, he directed the communications at issue solely to his friend group, which consisted of 100 people, or 0.00002% of the potential audience. The Commonwealth's proposal ignores that a person can be both popular and private. It

[6] There is also no dispute that the officer was able to accomplish that only by sending the defendant a friend request from a username that the court suggested was likely designed to "resonate with the audience that he was trying to . . . snoop on." See Tr.74:16-20. The Court should reject the Commonwealth's *ipso facto* argument that accepting the police officer's friend request demonstrates the defendant had no subjective expectation of privacy. The fact that the police deception succeeded in allowing their entry to the defendant's private space does not make that space public; it makes the entry a search. And, having successfully precluded discovery on the actual username chosen by police, the Commonwealth cannot now argue that the defendant's acceptance of that username as a friend was constitutionally meaningful, nor can this Court draw any conclusion about the defendant's state of mind on that point, much less the negative inference that the Commonwealth seeks.

requires drawing artificial and arbitrary lines -- as demonstrated by applying simple math to the facts of this case. And the line sought by the Commonwealth creates a further constitutional dilemma because it squarely pits the right of individuals to associate freely against the right of individuals to communicate privately with the associates they choose.

The clearest line to draw between public and private communications on social media is the same common-sense line drawn by social media providers themselves: a post or communication that is open and accessible to all within a particular application is "public," and a post or communication that is sent or accessible to only a selected subset of people is "private." With regard to "private" communications, law enforcement cannot unilaterally take steps to listen in without the constitutional safeguards of probable cause and a warrant.

C. Prior Precedent on Police Ruses Does Not Authorize the Police Conduct at Issue Here.

The Commonwealth's alternate line of defense is to rely on cases approving of ruses employed by police in other contexts. Although law enforcement may use deceit in some circumstances, not every ruse is permissible under Article 14 or the Fourth Amendment. Even a cursory reading of the Commonwealth's cases show that they do not permit the police conduct at issue here.

The "ruse" line of cases dates back to *Lewis v. United States*, 385 U.S. 206, 206-207 (1966). In *Lewis*, a federal agent misrepresented his identity and entered

the defendant's home to buy drugs, and the defendant challenged the warrantless entry of his home under the Fourth Amendment. *Id.* at 208. The Court upheld the entry because the defendant's home had been "converted into a commercial center to which outsiders are invited for purposes of transacting unlawful business," the defendant invited the agent into his home "for the specific purpose of executing a felonious sale of narcotics," and the agent did not "see, hear, or take anything" while in the home other than the drugs petitioner sold him. *Id.* at 210-211. Such an undercover operation is a classic example of permissible deception.

Lewis distinguished those facts from *Gouled v. United States*, 255 U.S. 298 (1921), abrogated on other grounds by *Warden, Md. Penitentiary v. Hayden*, 387 U.S. 294 (1967), in which the Supreme Court "had no difficulty concluding that the Fourth Amendment had been violated." *Lewis*, 385 U.S. at 209-210. In *Gouled*, a person acting in concert with the government entered the defendant's office by "falsely representing that he intended only to pay a social visit," but then "ransacked the office and seized certain private papers of an incriminating nature." *Id.* *Lewis* specifically cautioned that its holding "does not mean that, whenever entry is obtained by invitation . . . an agent is authorized to conduct a general search for

incriminating materials; a citation to the *Gouled* case . . . is sufficient to dispose of that contention." *Id.* at 211.[7]

The "ruse" cases cited by the Commonwealth as purportedly supporting the police conduct here all follow the general principle enunciated in *Lewis*: police are permitted to use trickery to gain entry into places being used to commit crimes in order to accomplish limited law enforcement purposes -- but never for the purpose of conducting a warrantless, suspicionless search. In fact, most of the cases cited by the Commonwealth involved a warrant.[8] The remainder involved cases where the police either affirmatively identified themselves as law enforcement or entered commercial areas that were being used to commit crimes. See *Commonwealth v. Gaynor*, 443 Mass. 245, 253-254 (2005) (defendant's consent to provide blood samples was valid where he knew police would use sample to test evidence from murder victim); *Commonwealth v. D'Onofrio*, 396 Mass. 711, 717-718 (1986) (police officer could lie to gain access to unlawful commercial business because "police officers may accept a general public invitation to enter commercial premises,

[7] *Gouled*'s separate holding that the government may not seize property simply for the purpose of proving a crime, see *Gouled*, 255 U.S. at 309-311, was subsequently overruled. See *Warden, Md. Penitentiary v. Hayden*, 387 U.S. 294 (1967).

[8] In these cases, police used ruses to gain entry to protected spaces to execute the warrant. See *Commonwealth v. Kaupp*, 453 Mass. 102, 107-108 (2009); *Commonwealth v. Sepulveda*, 406 Mass. 180, 182-183 (1989); *Commonwealth v. Watson*, 36 Mass. App. Ct. 252, 258 (1994).

and while there . . . they may take note of anything in plain view" (quoting *Commonwealth v. Cadoret*, 388 Mass. 148, 150-151 (1983));[9] *cf. Commonwealth v. Yehudi Y.*, 56 Mass. App. Ct. 812, 815-816 (2002) (reversing denial of motion to suppress because although officers' entry into home to buy marijuana was proper, second entry during which warrantless search was conducted violated Fourth Amendment and Article 14).

This case is *Gouled*, not *Lewis*: the police entered a private, non-commercial digital space "by stealth" for the sole purpose of conducting a search. *Gouled*, 255 U.S. at 305. They never identified themselves as law enforcement or stated that the purpose of their friend request was to allow them to surveil and record the content of the defendant's private Snapchat communications on an ongoing basis. Their purpose was not the same as the "purposes contemplated by the occupant," *Lewis*, 385 U.S. at 211; police surveillance clearly fell outside of the contemplated social

[9] *D'Onofrio* affirmed the police conduct despite the fact that the police officer's misrepresentation rendered his entry a trespass, because it read *Katz* as doing away with the argument that trespass alone constitutes a Fourth Amendment violation. See *D'Onofrio*, 396 Mass. at 718. *D'Onofrio*, however, did not anticipate *Jones*. See *Jones*, 565 U.S. at 406-407 ("[F]or most of our history, the Fourth Amendment was understood to embody a particular concern for government trespass upon the areas . . . it enumerates. *Katz* did not repudiate that understanding."). Petitioner argues in this case that he had a property interest in the contents of his Snapchat account by virtue of Snapchat's terms of service, and that the fake identity used by the police to gain access to those contents constituted a trespass in violation of the Fourth Amendment and Article 14. See Br. of Def.-Appellant at 17-21. MACDL agrees with that argument, which establishes a separate and independent basis upon which to reverse the trial court in this case.

purpose of friendship on Snapchat. The defendant's Snapchat account was not an "unlawful commercial business" like in *D'Onofrio* or *Lewis*; it was a means by which the defendant privately communicated with his friends. The police did not seek to enter the defendant's circle of friends for a limited purpose, like consummating an illegal transaction or executing a search warrant; they sought entry so that they could silently spy on every communication that the defendant sent to his friends as often and as long as they wanted. And unlike in any other case or context, the police ruse here has no temporal limitation because a virtual conversation never ends; once inside the defendant's circle of "friends," the police can simply sit back and surveil every subsequent communication forever more.[10] The Commonwealth fails to cite any cases that support affirmance on these facts, because none do. Police cannot use a ruse to rummage around in the private space of someone they suspect

[10] Concerns about law enforcement deception are at their zenith on the Internet because an online ruse is far easier to accomplish than a real-world one. Fake social media accounts frequently lure people into believing the account represents a real-world person they know and trust, and people commonly accept new friends on social media by looking to imperfect means of verification such as whether they have friends in common. Young people in particular are more vulnerable to trickery in the virtual world. See, e.g., Amanda Lenhart et al., *Teens, Technology & Friendships*, Pew Rsch. Ctr. 2 (Aug. 6, 2015), available at https://www.pewresearch.org/internet/2015/08/06/chapter-4-social-media-and-friendships/; Caitlin R. Costello, M.D., et al, *Adolescents and Social Media: Privacy, Brain Development, and the Law*, 44 J. Am. Acad. Psychiatry & Law 313, 313-321 (2016).

of nothing, and a ruse entry does not authorize a "general search for incriminating materials." *Lewis*, 385 U.S. at 211.

D. Using Electronic Devices to Surveil and Record the Defendant's Private Communications Violated Clearly Established Constitutional and Statutory Law.

The facts also bring this case squarely within cases decided by this Court and the United States Supreme Court holding that the government cannot use electronic means to surreptitiously spy on people without probable cause and a warrant. See, e.g., *Blood*, 400 Mass. at 70; see also *Katz*, 389 U.S. at 353; *Silverman v. United States*, 365 U.S. 505, 511 (1961).

Indeed, the police conduct in this case may well have violated the wiretap statute, Mass. G. L. c. 272, § 99(B)(4), which proscribes secretly hearing or recording the contents of any wire or oral communication without (1) prior authority by all parties to the communication; or (2) a judicially issued warrant, unless the party secretly conducting the recording is a law enforcement officer investigating a designated offense who is either a party to the communication or has advance authorization from a party to conduct the interception. See *Commonwealth v. Tavares*, 459 Mass. 289, 297-298 (2011). There is no evidence that the defendant was being investigated for a "designated offense," or even that he was under investigation at all when this surveillance began; the police were only parties to the conversation through trickery; and they had no advance authorization from any party

or a court to conduct these interceptions. See Mass. G. L. c. 272, § 99(A) ("[T]he uncontrolled development and unrestricted use of modern electronic surveillance devices pose grave dangers to the privacy of all citizens[.] . . . The use of such devices by law enforcement officials must be conducted under strict judicial supervision and should be limited to the investigation of organized crime.").

The concerns animating these laws are particularly applicable in a case like this one, where the social media platform at issue (Snapchat) is specifically designed to not make a permanent record and users are specifically encouraged to expect that their Snapchat communications will function "like talking to someone in person or on the phone . . . ." See Snaps & Chats, available at https://www.snap.com/en-US/privacy/privacy-by-product. In this case, the police lurked in the defendant's friend list so they could surveil and record what he was saying for possible use against him. Those actions render this case indistinguishable from *Katz*, *Blood*, or any other electronic surveillance case, and render the officer's conduct plainly unconstitutional.

E. Article 14 and the Fourth Amendment Do Not Permit Unfettered Surveillance of the Content of Private Communications.

Precluding the limitless, suspicionless, warrantless surveillance employed by the police in this case does not mean that social media communications operate in a "police free" zone. There are clearly risks inherent in sharing private information with others -- just as there are risks that someone will follow your car on a public

street. A false friend can always take information that was sent or posted privately and provide it to others, including the police, and if that had happened here, it would be a much different case. See, e.g., *Commonwealth v. Snow*, 96 Mass. App. Ct. 672, 675-676 (2019) (information provided by third party about defendant's social media use led to review of victim's cell phone and warrant to search defendant's cell phone, which in turn recovered Snapchat video recordings), aff'd 486 Mass. 582 (2021). But that is not what happened here. No one betrayed the defendant's confidences by providing his information to the police. The police themselves surreptitiously gained access to the Snapchat account he used to communicate privately with his selected associates, and thereafter monitored and recorded those communications for a month with no limits, standards, or oversight.

The mere possibility that one of the defendant's friends might have disclosed these communications to the police cannot defeat his expectation of privacy in them, as the Supreme Court has long held. See *United States v. Karo*, 468 U.S. 705, 716 n.4 (1984) ("[T]here would be nothing left of the Fourth Amendment right to privacy if anything that a hypothetical government informant might reveal is stripped of constitutional protection. . . . [T]here is a substantial distinction between revelations to the Government by a party to conversations with the defendant and eavesdropping

on conversations without the knowledge or consent of either party to it.") (emphasis added) (quotations and internal punctuation omitted).[11]

"[W]hether privacy expectations are legitimate within the meaning of *Katz* depends not on the risks an individual can be presumed to accept when imparting information to third parties, but on the risks he should be forced to assume in a free and open society." *Smith v. Maryland*, 442 U.S. at 750 (Marshall, J. dissenting). There is a substantial difference between what can happen and what people reasonably expect to happen. "Courts should bear in mind that the issue is not whether it is *conceivable* that someone could eavesdrop on a conversation but whether it is *reasonable* to expect privacy." *United States v. Smith*, 978 F.2d 171,

[11] This Court's decision in *Commonwealth v. Delgado-Rivera*, 487 Mass. 551 (2021), does not change this analysis. There, the Court held that a sender of text messages has no standing to challenge a search of those messages on the recipient's phone, reasoning that the sender assumes the risk that the recipient might reveal the text messages to the police. *Id*. at 561. But "assumption of risk" principles apply only when police obtain information from a third party source. See *Karo*, 468 U.S. at 716 n.4 ("assumption of risk" principles only apply in cases involving a third-party source; otherwise "it could easily be said that . . . Katz had no reasonable expectation of privacy in his conversation because the person to whom he was speaking might have divulged the contents of the conversation"). *Delgado-Rivera* also noted the distinctions between text messaging and "encrypt[ed] or ephemeral messaging" applications like Snapchat, see *Delgado-Rivera*, 487 Mass. at 561 n.7, and the latter does evince a greater expectation of privacy. Unlike text messaging, Snapchat does not "create[] a memorialized record of the communication that [is] beyond the control of the sender," *id*. at 560, and Snapchat expressly markets this feature to its users. See Our Privacy Principles, available at https://www.snap.com/en-US/privacy/privacy-center ("Snapchat aims to capture the feeling of hanging out with friends in person – that's why Snaps and Chats are deleted from our servers once they're opened or expired.").

179 (5th Cir. 1992) (emphasis in original). Here, social media users do not expect that the police will surveil and record their communications with friends, and no court would accept as constitutional a practice by which law enforcement offered themselves as "friends" to each of the millions of Americans on social media and thereafter monitored and limitlessly surveilled the private postings of those not sufficiently "paranoid" to decline the invitation -- yet that is exactly the Pandora's Box that would open if this Court were to affirm the police conduct in this case. See, e.g., *Blood*, 400 Mass. at 73 n.13; *Mora*, 485 Mass. at 367.

The burden of this police practice is not borne by criminal defendants alone. "The relevant question is not whether criminals must bear the risk of warrantless surveillance, but whether it should be imposed on all members of society." *Blood*, 400 Mass. at 73 (quotations and internal punctuation omitted). The rulings that the Commonwealth seeks place the onus on each of us to individually guard against the possibility of warrantless, suspicionless government surveillance of our private communications on social media -- a result that would simultaneously permit a breathtaking expansion of police power and repudiate bedrock principles on which our society was established.

Moreover, the power the Commonwealth attempts to claim for the police is as effortless as it is intrusive. "In the precomputer age, the greatest protections of privacy were neither constitutional nor statutory, but practical. Traditional

surveillance for any extended period of time was difficult and costly and therefore rarely undertaken." *Jones*, 565 U.S. at 429 (Alito, J., concurring in judgment). Today, however, the police can easily send one-click friend requests to as many people as they want -- regardless of the presence or absence of individualized suspicion. And once those requests are accepted, the police can infiltrate social circles for all time, monitoring and recording messages meant only for friends from the comfort of their own computer or smartphone. Unlike searches of physical space that occur in the real world, this sort of digital surveillance makes "long-term monitoring relatively easy and cheap." *Id*. The absence of a practical constraint on an intrusive police surveillance practice demands a constitutional one, as this Court has recognized. *Commonwealth v. McCarthy*, 484 Mass. 493, 500 (2020) (citation omitted).

Warrantless, suspicionless, unfettered electronic surveillance of Massachusetts residents' private communications is unconstitutional under Article 14 and the Fourth Amendment -- regardless of whether those communications take place by telephone, email, text, or social media. Where, as here, a person shares information to a select group of associates and not to the public at large, that person has exhibited a reasonable expectation of privacy as against all other listeners. Disclosure to one's friends is not disclosure to the world, and ongoing government

surveillance of private communications may take place only with probable cause and a warrant.

II. The Police Practice at Issue Here Carries Additional Constitutional Problems Under Articles 1, 10, and 16 of the Declaration of Rights and the First, Fifth, and Fourteenth Amendments to the U.S. Constitution.

The police conduct at issue here additionally threatens our rights to freely associate and speak as guaranteed by Article 16 and the First Amendment. "[P]ervasive monitoring chills associational and expressive freedom and allows the government to assemble data that reveal private aspects of identity, potentially altering the relationship between citizen and government in a way that is inimical to democratic society." *Rousseau*, 465 Mass. at 381 (citing *Jones*, 565 U.S. at 416) (quotation and citation omitted).[12] Moreover, there is a real concern that the police are surveilling private Snapchat communications in a racially discriminatory manner in violation of Articles 1 and 10 and the Fifth and Fourteen Amendments. See *Commonwealth v. Dilworth*, Nos. 1884CR00453, 1884CR00469, 2019 WL 469356, *4 (Mass. Super. Ct. Jan. 18, 2019), aff'd *Commonwealth v. Dilworth*, 485 Mass. 1001 (2020). These concerns highlight the wrongfulness of the police conduct in

[12] See also *U.S. Dist. Ct.*, 407 U.S. at 314 (warrantless government eavesdropping of private communications not permitted because "[p]rivate dissent, no less than open public discourse, is essential to our free society"); *Shelton v. Tucker*, 364 U.S. 479, 485-486 (1960) (unconstitutional to compel teachers to disclose their associational ties); *NAACP v. Alabama*, 357 U.S. 449, 462-463 (1958) (same for NAACP membership list).

this case, and the risks attendant with permitting this type of surveillance without the constitutional safeguards of probable cause and a warrant.

CONCLUSION

For the foregoing reasons, this Court should reverse the Superior Court's decision, and hold that the police must establish probable cause and obtain a warrant before they can monitor or record private communications sent via social media accounts.

Dated: August 18, 2021

Respectfully submitted,

/s/ Sara E. Silva

Sara E. Silva (BBO #645293)
Hogan Lovells US, LLP
125 High Street, Suite 2010
Boston, MA 02110
(617) 371-1000
sara.silva@hoganlovells.com

CERTIFICATION OF COMPLIANCE

I, Sara E. Silva, certify that this brief complies with the Rules of Court that pertain to the filing of amicus briefs, including but not limited to Rules 16, 17, and 20. This brief complies with the length limit because it is set in 14-point proportionally spaced font and contains 7,491 non-excluded words, as determined through use of the "word count" feature in Microsoft Word 2010.

/s/ Sara E. Silva
Sara E. Silva (BBO #645293)

CERTIFICATE OF SERVICE

I, certify under the penalties of perjury that on August 18, 2021, a copy of the foregoing document was filed electronically through the Court's e-filing system for service to the following registered attorneys:

Suzanne Lynn Renaud
11 Robert Toner Blvd.
Suite 5 #186
North Attleboro, MA 02760
(508) 399-1060

Ian MacLean
Office of the District Attorney/Suffolk County
One Bulfinch Place
Boston, MA 02114
(617) 619-4081

/s/ Sara E. Silva
Sara E. Silva (BBO #645293)