19-P-944 Appeals Court

COMMONWEALTH vs. MALCOLM McMANN.

No. 19-P-944.

Worcester. January 30, 2020. - June 3, 2020.

Present: Wolohojian, Milkey, & Shin, JJ.

Abuse Prevention. Cellular Telephone. Social Media. Evidence, Authentication. Practice, Criminal, Required finding.

Complaint received and sworn to in the Worcester Division of the District Court Department on September 25, 2017.

The case was heard by Paul F. LoConto, J.

Joseph Visone for the defendant.
Abigail H. Salois, Assistant District Attorney, for the Commonwealth.

SHIN, J. After a jury-waived trial, the defendant was convicted of violating an abuse prevention order. See G. L. c. 209A, § 7. At issue is whether the evidence was sufficient to prove beyond a reasonable doubt that the defendant was the

person who sent the Instagram message[1] that was the basis for the conviction. We conclude that it was not and therefore reverse.

Background. The judge could have found the following facts. After dating the defendant for approximately five months, the victim obtained an abuse prevention order against him. The order prohibited the defendant from, among other things, contacting the victim "in writing, electronically or otherwise, either directly or through someone else."

While the order was in effect, the victim received an Instagram message from the username "bigm617." The message said simply, "Yoooo." The victim testified that she knew "bigm617" was the defendant's username because the associated account displayed pictures of the defendant, including one of him with the victim, and the victim and the defendant had previously "liked" and commented on each other's Instagram posts.

The victim went to the police station and, using her cell phone, showed the Instagram message to an officer. Later that night the defendant met with the same officer and denied sending any message to the victim. According to the officer, the defendant "wanted to show me that he never did" and entered a passcode to unlock his cell phone. He then opened the Instagram

[1] Instagram, which can be downloaded as a cell phone application, is a social media platform that enables users to share photographic content and send messages to other users.

application on his cell phone, and the "Yoooo" message to the victim appeared on the screen. The officer observed that the defendant looked "[s]urprised."

Discussion. "We consider whether, after viewing the evidence in the light most favorable to the Commonwealth, any rational trier of fact could have found the essential elements of the crime[] beyond a reasonable doubt." Commonwealth v. Ayala, 481 Mass. 46, 51 (2018). To sustain a conviction under G. L. c. 209A, § 7, the Commonwealth has the burden of proving, among other elements, that the defendant violated an abuse prevention order. See Commonwealth v. Telcinord, 94 Mass. App. Ct. 232, 235 (2018). Thus, here, we must determine whether the judge could find proof beyond a reasonable doubt that the defendant was the person who contacted the victim by sending her the Instagram message.

We are guided by cases addressing electronic communications in the authentication context. Even under the lower preponderance of the evidence standard that applies to authentication, see Commonwealth v. Oppenheim, 86 Mass. App. Ct. 359, 366-367 (2014), "[e]vidence that the defendant's name is written as the author of an e-mail or that the electronic communication originates from an e-mail or a social networking Web site . . . that bears the defendant's name is not sufficient alone to authenticate the electronic communication as having

been authored or sent by the defendant." Commonwealth v. Purdy, 459 Mass. 442, 450 (2011). Rather, there must be additional circumstantial evidence of the source of the communication, such as evidence regarding the security of the account. See id. at 450-451 ("e-mails were authenticated as having been authored by the defendant" where they "originated from an account bearing the defendant's name and acknowledged to be used by the defendant" and "were found on the hard drive of the computer that the defendant acknowledged he owned, and to which he supplied all necessary passwords"). Other circumstantial evidence may include "[t]he appearance, contents, substance, internal patterns, or other distinctive characteristics of the item." Mass. G. Evid. § 901(b)(4) (2019). See Purdy, supra at 447-448.

Commonwealth v. Williams, 456 Mass. 857 (2010), provides a useful analogy. At issue there was whether the Commonwealth authenticated messages sent from a "MySpace" account that the recipient of the messages identified as belonging to the defendant's brother. Although the account bore a picture of the defendant's brother, and the messages themselves displayed some familiarity with the recipient, id. at 868, the court held that the Commonwealth failed to prove the source of the messages, because "while the foundational testimony established that the messages were sent by someone with access to [the] MySpace Web

page, it did not identify the person who actually sent the communication." Id. at 869. For example, there was no testimony about "how secure such a Web page is, who can access a My[S]pace Web page, [or] whether codes are needed for such access." Id.

Here, even assuming without deciding that the Instagram message was properly authenticated, the Commonwealth failed to meet its higher burden of proving beyond a reasonable doubt that the defendant was the person who wrote or sent the message to the victim. Although the evidence was sufficient to show that the Instagram account was the defendant's and that he could access it, there was no circumstantial evidence establishing authorship. Nothing about the content or tone of the message, "Yoooo," corroborated that the defendant wrote it. The message did not refer to any prior conversation between the parties or contain other distinctive characteristics. Cf. Oppenheim, 86 Mass. App. Ct. at 368 (evidence sufficient to authenticate that defendant wrote instant message, where tone was familiar to recipient, and message referred to earlier discussions with recipient and personal details about defendant). In fact, contrary to the Commonwealth's assertion, the evidence did not

even show that the defendant previously sent the victim messages through Instagram.[2]

Furthermore, as in Williams, 456 Mass. at 869, the evidence did not establish any limitations on who could access the defendant's Instagram account.[3] There was no evidence that users generally, or the defendant specifically, must enter a password to access Instagram.[4] While certain questions posed by the Commonwealth assumed the requirement of a password, "[c]ounsel's

---

[2] On direct examination the Commonwealth asked the victim, "And before you had your restraining order, you had previously talked to the defendant on Instagram messenger . . . using this name?" While the victim answered, "Yes," no evidence was offered to explain the meaning of "Instagram messenger." It is unclear whether the Commonwealth was referring to Instagram generally or a feature or application; if the latter, there was no evidence regarding how such a feature or application works or even whether something called "Instagram messenger" exists. Moreover, in response to the follow-up question -- "[H]ow often would you say you communicated with the defendant via Instagram?" -- the victim stated only, "We liked each other's posts." Then, on cross-examination, the victim confirmed that her Instagram communication with the defendant was limited to "liking posts and comments."

[3] We do not preclude the possibility that evidence regarding the security of an account could alone be sufficient to prove authorship. See, e.g., Purdy, 459 Mass. at 450-451 (preponderance standard). Nor do we preclude the possibility that a c. 209A violation could be established through evidence that a defendant failed to secure his or her social media account after being put on notice that it had been used to contact the person holding the c. 209A order. But here, the Commonwealth offered no such evidence.

[4] The Commonwealth acknowledged at oral argument that this would not be an appropriate subject of judicial notice.

questions are not evidence." Commonwealth v. Gomez, 450 Mass. 704, 713 (2008). Nor was there evidence about how regularly the defendant may have needed to enter a password to access his account. See Sublet v. State, 442 Md. 632, 661-662 (2015) ("Unauthorized access of a [social networking] profile can occur even without password sharing when an individual remains logged in to his or her account through their cell phone or computer and leaves them unattended, thereby allowing third parties access to the profile").

Although the Commonwealth cites the fact that the defendant needed a passcode to open his cell phone, this does not tip the scale in favor of sufficiency because the Commonwealth offered no evidence that a cell phone is the only, or even primary, means of accessing an Instagram account. In fact, the officer testified that Instagram accounts can be accessed from multiple devices, such as tablets and desktop computers. The Commonwealth also put in no evidence to show (nor does it argue on appeal) that a message appearing on an Instagram cell phone application is akin to a text message on a cell phone or to an e-mail downloaded to a computer hard drive.[5] Cf. Purdy, 459

[5] Defense counsel tried to explain this distinction in response to the judge's question, "The message itself is not on the phone?" During this discussion the judge acknowledged that he was "not familiar with Instagram." Later, he commented to the Commonwealth, "You know, you are assuming that the fact

Mass. at 450-451. Thus, that the message appeared when the defendant opened the Instagram application is not proof that he used his cell phone to send it. The Commonwealth conceded as much at oral argument.

Citing only Purdy, an authentication case, the Commonwealth argues that the conviction should be affirmed because there was no evidence that anyone else knew the defendant's Instagram password (assuming he needed one) or could otherwise access his account. Purdy is factually distinguishable, however, because the e-mails at issue there were found on the hard drive of the defendant's computer, which was password-protected. See Purdy, 459 Mass. at 450-451. More fundamentally, even assuming that the Instagram message here was properly authenticated (again, an issue we do not decide), it was the Commonwealth's burden to prove beyond a reasonable doubt all the elements of the offense, including that the defendant violated the abuse prevention order by sending the message to the victim. See Commonwealth v. Meola, 95 Mass. App. Ct. 303, 314-316 (2019) (concluding that Facebook message was authenticated and going on to determine whether message and accompanying video were sufficient to prove beyond reasonable doubt that defendant purposefully disseminated

---

finder understands all of this. I think you have to lay a foundation."

matter harmful to minor). The Commonwealth failed to meet its burden either through evidence that the message itself contained characteristics showing that the defendant wrote it, or through evidence establishing how secure Instagram accounts are and how the Instagram cell phone application works.[6] The defendant's motion for a required finding of not guilty should therefore have been allowed. See Commonwealth v. Cove, 427 Mass. 474, 476 (1998) ("Commonwealth did not prove an essential element of the crime, namely, the 'contacting' of [the victim]").

Judgment reversed.

Finding set aside.

Judgment for defendant.

[6] We note that, in the face of the judge's admitted lack of familiarity with Instagram, and his apparent confusion about whether a message that appears on the Instagram application is on the cell phone itself, the Commonwealth nonetheless suggested in closing that the message was akin to a text message on a phone: "[T]hat day when [the defendant] was asked about that violation of the restraining order, he brought out his phone, a password protected phone, entered his password. Opened the application of Instagram. Went to his own personal messages on his own personal phone. Went to the messages of [the victim] and . . . the officer saw with his own eyes the message that [the victim] had brought earlier that day, the 'Yo' message that came in at 1:07 a.m." As discussed, there was no evidence to support such a comparison, as the Commonwealth concedes on appeal.