18-P-83 Appeals Court

COMMONWEALTH vs. URBANO MEOLA.

No. 18-P-83.

Middlesex. November 1, 2018. - May 22, 2019.

Present: Agnes, Blake, & Neyman, JJ.

Obscenity, Dissemination of obscene matter to minor. Social Media. Evidence, Authentication, Digital image. Practice, Criminal, Motion for a required finding.

Complaint received and sworn to in the Malden Division of the District Court Department on August 18, 2016.

The case was heard by Joseph W. Jennings, III, J.

Mehmet Baysan for the defendant.
Benjamin Lees (Kevin J. Curtin, Assistant District Attorney, also present) for the Commonwealth.

AGNES, J. The defendant, Urbano Meola, appeals from his conviction, following a jury-waived trial, of dissemination of obscene material to a minor in violation of G. L. c. 272, § 28. The defendant argues that the judge erroneously admitted in

evidence a Facebook message[1] and the accompanying video attached to the message that was sent to the victim, the then seventeen year old daughter of his former live-in girlfriend. The video depicted the defendant seated and unclothed, rubbing his penis and his anus.[2] For the reasons explained infra, the evidence before the judge was sufficient to authenticate the Facebook message as a digital communication sent to the victim by the defendant. See Mass. G. Evid. § 901(b)(4), (11) (2019). Furthermore, we conclude that because the evidence presented by the Commonwealth was sufficient to permit the judge to conclude beyond a reasonable doubt that the defendant sent the video to the victim, the judge did not err in denying the defendant's motion for a required finding filed at the close of the Commonwealth's case.

Background. Viewing the evidence in the light most favorable to the Commonwealth, the judge could have found the following facts. The defendant and the victim's mother were in a relationship for approximately nine years, ending in 2009. In

---

[1] "Members [of social networking websites such as Facebook and MySpace] create their own individual web pages (their profiles) on which they post their own personal information, photographs and videos, and from which they can send and receive messages to and from others whom they have approved as their 'friends.'" 2 McCormick on Evidence § 227, at 20 (2013 & Supp. 2016).

[2] The video was marked Exhibit 1 and is part of the record on appeal.

2005, they had one daughter together, the victim's half-sister.[3] The defendant and the mother never married, although they lived together with the children and were at one time engaged. The victim was seventeen years old at the time of the events giving rise to this case. Neither the mother nor the children had any contact with the defendant from the time the adults separated until this incident.[4]

On August 12, 2016, the victim received a message notification on her cell phone from her Facebook account that read: "You have a message request from Urbano Meola." There was no text otherwise accompanying the notification, but rather "just a screen that said 'play,'" alerting the victim that the entirety of the communication was a video.

The victim testified that she was "freaked out" and "nervous" upon receiving the message because she and the defendant had not communicated in any way since his relationship with her mother had ended at least six years prior, and because she and the defendant were not "friends" on Facebook. The account that sent the video bore the defendant's name and a

---

[3] The defendant was not the victim's father.

[4] There was evidence that several years after their relationship ended, the mother went to the Department of Revenue in an effort to collect child support from the defendant. However, she testified that nothing came of it because "we didn't know where he was."

profile picture of the victim's younger half-sister, the defendant's daughter.[5] Later that evening, the victim watched the thirty-second video, which, as noted above, depicts the defendant seated and unclothed, rubbing his penis and his anus. Within a day or two, the victim received a "friend request" via Facebook from the same account that had sent the video of the defendant.

In addition to this testimony from the mother and the victim, the judge heard testimony from Everett Police Officer Nicole O'Donnell, who viewed the video of the defendant on the victim's phone and wrote a police report. Everett Police Detective Nicholas Crowell also testified. He spoke to the victim's aunt, who had accompanied the victim to the police station and had forwarded the video to him via an e-mail message (e-mail). Detective Crowell described the video in question as a "thirty-one-second video of a male showing his genitalia area. It's viewed from down below, looking up towards the person in the video." After speaking with Officer O'Donnell, Detective Crowell identified the male in the video as the defendant based on a photograph he had obtained from the registry of motor vehicles. On August 17, 2016, the defendant was arrested in his

[5] There is no evidence that further describes the photograph of the victim's half-sister. While the photograph was the subject of oral testimony, it was not introduced in evidence.

room at a rooming house in Revere. No computers, cell phones or digital devices were in the defendant's room or on his person at the time of his arrest, and neither the police nor the Commonwealth ever sought to obtain a search warrant seeking any electronic devices owned by or accessible to the defendant.

The judge admitted into evidence the video the victim had received. However, finding that the prosecutor had failed to comply with the requirement of Mass. R. Crim. P. 17 (a) (2), 378 Mass. 885 (1979), that, prior to trial, subpoenaed records must be delivered to the clerk's office, the judge excluded records proffered by the prosecutor and described as user information relating to the Facebook account of the person who had sent the video (Facebook account records).

Discussion. General Laws c. 272, § 28, provides, in pertinent part, that "[w]hoever purposefully disseminates to a person he knows or believes to be a minor any matter harmful to minors, as defined in [G. L. c. 272, § 31], knowing it to be harmful to minors, . . . shall be punished . . . ." The term "purposely" is generally understood to mean deliberately or intentionally, as opposed to accidentally.[6] The term "matter," as used in § 28, is defined broadly and includes a video like

[6] Compare "purposeful," defined as "having a purpose: as (a) meaningful, (b) intentional." Merriam-Webster's Collegiate Dictionary 1011 (11th ed. 2005). Cf. Commonwealth v. York, 9 Met. 93, 105 (1845) (defining malice).

the one involved in this case.[7] The term "disseminates," as used in § 28, also is defined broadly and includes circumstances in which a video is attached to a Facebook message and transmitted electronically to another Facebook subscriber as happened in this case.[8] The term "knowing," as used in § 28, is defined as "a general awareness of the character of the matter." G. L. c. 272, § 31. Finally, "harmful to minors," as used in § 28, includes matters which meet the definition of obscenity.[9]

---

[7] The term "matter" is defined in G. L. c. 272, § 31, as follows:

> "[A]ny handwritten or printed material, visual representation, live performance or sound recording including, but not limited to, books, magazines, motion picture films, pamphlets, phonographic records, pictures, photographs, figures, statues, plays, dances, or any electronic communication including, but not limited to, electronic mail, instant messages, text messages, and any other communication created by means of use of the Internet or wireless network, whether by computer, telephone, or any other device or by any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photo-electronic or photo-optical system."

[8] The term "disseminates" is defined in G. L. c. 272, § 31, as "to import, publish, produce, print, manufacture, distribute, sell, lease, exhibit or display."

[9] The phrase "harmful to minors" is defined in G. L. c. 272, § 31, as follows:

> "[M]atter is harmful to minors if it is obscene or, if taken as a whole, it (1) describes or represents nudity, sexual conduct or sexual excitement, so as to appeal predominantly to the prurient interest of minors; (2) is patently contrary to prevailing standards of adults in the county where the offense was committed as to suitable

The defendant did not object to the testimony by the mother and the victim that the person in the video was the defendant, and no question in that regard is raised on appeal.[10] The defendant does not question that the video was disseminated to the victim, or that it was a matter that is harmful to minors, within the meaning of G. L. c. 272, § 28. Rather, the defendant argues on appeal that the video and the communication that it was attached to were admitted without a proper evidentiary foundation because the Commonwealth failed to authenticate the digital message containing the video as a message purposefully sent by him.

1. Authentication as a condition of relevance. "The general rule to be followed in this Commonwealth is that all relevant evidence is admissible unless within an exclusionary rule. Evidence is relevant if it renders the desired inference more probable than it would be without the evidence." Poirier

---

material for such minors; and (3) lacks serious literary, artistic, political or scientific value for minors."

[10] The defendant did object prior to trial to any identification testimony by either of the police officers who testified. Detective Crowell testified over objection that he located the person depicted in the video by examining a registry of motor vehicles photograph of the defendant. We construe the judge's ruling in context as admitting the evidence for the limited purpose of explaining how the police came into contact with the defendant. See Commonwealth v. Cordle, 404 Mass. 733, 743-744 (1989). In any case, at trial and in his closing argument, the defendant did not dispute that he is the person depicted in the video.

v. Plymouth, 374 Mass. 206, 210 (1978).[11] "Authentication represents a special aspect of relevancy in that evidence cannot have a tendency to make the existence of a disputed fact more or less likely if the evidence is not that which its proponent claims" (citations and quotation omitted). United States v. Branch, 970 F.2d 1368, 1370 (4th Cir. 1992). For this reason, authentication of digital evidence such as an e-mail, an electronic message using a social media platform, a screenshot from a website, or a videotape recording "is a condition precedent to its admissibility." Commonwealth v. Foster F., 86 Mass. App. Ct. 734, 737 (2014).[12]

---

[11] In order to be admissible at trial, relevant evidence must, of course, make a fact of consequence in the proceeding more or less probable. Harris-Lewis v. Mudge, 60 Mass. App. Ct. 480, 485 (2004). See Mass. G. Evid. § 401 (2019).

[12] See, e.g., Commonwealth v. Caruso, 476 Mass. 275, 291 (2017) (error to admit certain screen shots from defendant's computer because there was no foundational evidence indicating that "the defendant had ever accessed the information depicted in the screen shots"); Commonwealth v. Purdy, 459 Mass. 442, 450-451 (2011) (judge properly admitted series of e-mail exchanges based on "this threshold: in addition to the e-mails having originated from an account bearing the defendant's name and acknowledged to be used by the defendant, the e-mails were found on the hard drive of the computer that the defendant acknowledged he owned, and to which he supplied all necessary passwords"); Commonwealth v. Williams, 456 Mass. 857, 868–869 (2010) (electronic MySpace message inadmissible where proponent provided no foundation identifying who sent message); Commonwealth v. Connolly, 91 Mass. App. Ct. 580, 586-588 (2017) (police officer's testimony about contents of missing surveillance video should not have been admitted because Commonwealth did not lay sufficient foundation to demonstrate that video was genuine representation of events that occurred on

With regard to the authentication of evidence, the judge has a gatekeeper role, which requires the judge to assess the evidence and determine whether the jury or judge, acting as the fact finder, could find that the item in question is what its proponent claims it to be. See Mass. G. Evid. § 104(b) (2019).[13]

---

night in question); Commonwealth v. Gilman, 89 Mass. App. Ct. 752, 758-759 (2016) (Facebook chat conversations sufficiently authenticated based on evidence that they originated from account bearing defendant's name and including his photograph, and were found on hard drive of two laptop computers issued to defendant by his employer with access limited to defendant by use of user name and password). See also Mass. G. Evid. § 901(a), (b)(11) (2019). See generally Tienda v. State, 358 S.W.3d 633, 638 (Tex. Crim. App. 2012).

[13] "The role of judge as 'gatekeeper' is essential to authentication, because of jurors' tendency, 'when a corporal object is produced as proving something, to assume, on sight of the object, all else that is implied in the case about it,' for which Wigmore provided the following example:

> 'It is easy for a jury, when witnesses speak of a horse being stolen from Doe by Roe, to understand, when Doe is proved to have lost the horse, that it still remains to be proved that Roe took it; the missing element can clearly be kept separate as an additional requirement. But if the witness to the theft were to have a horse brought into the courtroom, and to point it out triumphantly, "If you doubt me, there is the very horse!", this would go a great way to persuade the jury of the rest of his assertion and to ignore the weakness of his evidence of Roe's complicity. The sight of the horse, corroborating in the flesh, as it were, a part of the witness' testimony, tends to verify the remainder.' [7 J.] Wigmore, [Evidence] § 2129 [(Chadbourn Rev. 1978)]." (Emphasis omitted.)

Sublet v. State, 442 Md. 632, 656 (2015).

Cases sometimes refer to the gatekeeper's determination as a preliminary finding of fact under Massachusetts law, reflected in Mass. G. Evid. § 104(b), as well as under Federal law, see

In the case of a digital communication that is relevant only if authored by the defendant, a judge is required to determine whether there is sufficient evidence to persuade a reasonable trier of fact that it is more likely than not that the defendant was the author of the communication. See Commonwealth v. Purdy, 459 Mass. 442, 447 (2011); Commonwealth v. Oppenheim, 86 Mass. App. Ct. 359, 366-367 (2014). We review a judge's preliminary determination of conditional relevancy under Mass. G. Evid. § 104(b) under an abuse of discretion standard. See Commonwealth v. Leonard, 428 Mass. 782, 786 (1999) ("these preliminary determinations are committed to the sound discretion of the judge . . . [whose] decision will be upheld on appeal absent palpable error" [quotation and citation omitted]). That standard means that we will not disturb the judge's ruling absent a clear error of either law or "judgment in weighing the relevant factors." Commonwealth v. Brown, 477 Mass. 805, 820

Fed. R. Evid. 104(b) (2019). However, it is more accurate to describe the judicial function under § 104(b) as a preliminary assessment or screening of the evidence, because the judge does not make a determination of credibility under § 104(b). "In determining whether the Government has introduced sufficient evidence to meet Rule 104(b), the trial court neither weighs credibility nor makes a finding that the Government has proved the conditional fact by a preponderance of the evidence. The court simply examines all the evidence in the case and decides whether the jury could reasonably find the conditional fact . . . by a preponderance of the evidence." Huddleston v. United States, 485 U.S. 681, 690 (1988).

(2017), citing L.L. v. Commonwealth, 470 Mass. 169, 185 n.27 (2014).

2. Admission of the Facebook account records. Prior to trial, the defendant objected to the Commonwealth's motion in limine to admit Facebook account records pertaining to "an account registered to Urbano Meola" and obtained by the Commonwealth pursuant to a subpoena for business records directed to Facebook under Mass. R. Crim. P. 17. In particular, the defendant argued that the records in question were not "certified," because there was no affidavit from a keeper of the records or a witness who would identify them as business records maintained by Facebook. In response, the prosecutor explained that a request for the records had been made to Facebook via the Internet through the Facebook "online request system," asking that the records be delivered to the court clerk's office. The prosecutor indicated that she had a copy of the records, and she assumed a copy was in the clerk's office.[14] However, there was

[14] The prosecutor further explained, "I know that the policy of Facebook is, being a newer company, they sent a basically encrypted link to us to allow us to access them, and my understanding is that that link was also sent to the clerk's office. Whether or not the clerk's office opened it, I'm not sure." Later, the judge reported that the "clerk's office does not have any envelopes regarding the defendant. I don't know that that's specifically what you said would have happened. . . . They would have sent some type of electronic communication to the court?" The prosecutor responded affirmatively, "because that is what the Commonwealth received. And our request and the order was that it be sent to the clerk's

neither a showing that such records were received by the clerk's office nor any evidence to support their authentication. Without resolving the disagreement over whether the Facebook account records had been authenticated, the judge ruled that the records in question were not admissible because the Commonwealth did not comply with rule 17. See Commonwealth v. Hart, 455 Mass. 230, 243 (2009) (when records are subpoenaed before trial pursuant to Mass. R. Crim. P. 17 [a] [2], record keeper must deliver them to clerk's office; thereafter, judge may allow parties and their attorneys to inspect and copy them; such records should not be delivered directly to requesting party).

On appeal, the Commonwealth does not take issue with this ruling.[15] The question before us thus becomes whether the judge abused his discretion or committed palpable error in determining that, even without the benefit of the Facebook account records, a fact finder could find that it was more likely than not that the Facebook message was authentic and, in particular, that it was sent by the defendant.[16]

---

office, and we received it, and my understanding was that the clerk's office would also receive it."

[15] The Facebook account records were not marked for identification and are not part of the record before us.

[16] There was a separate requirement that the video be authenticated apart from the Facebook message. That requirement was satisfied by the direct evidence consisting of the testimony of the victim and others that she received the video as part of

3. Authentication of the Facebook message. The defense challenged the admission of the Facebook message by means of a pretrial motion in limine,[17] on grounds that there was an insufficient factual basis to establish that the message received by the victim to which the video was attached was a communication sent by the defendant. In Purdy, 459 Mass. 442, the Supreme Judicial Court clarified the test for authenticating digital evidence that is not self-authenticating[18] and where there is no direct evidence available.[19] First, Purdy makes it

---

a Facebook message and that the video depicted the defendant, Urbano Meola.

[17] "Motions in limine concerning the introduction or exclusion of purportedly relevant evidence are properly made and considered before and during trial, in advance of the evidence being offered." Commonwealth v. Spencer, 465 Mass. 32, 42 (2013). See Mass. G. Evid. § 103(f) (2019).

[18] Self-authenticated documents include copies of documents recorded or filed in a public office and bearing "the attestation of the officer who has charge of the item . . . ." Mass. G. Evid. § 901(b)(7)(B) (2019).

[19] There is direct evidence of authentication where, for example, someone with personal knowledge testifies that an item is what it is claimed to be. See Commonwealth v. LaCorte, 373 Mass. 700, 704 (1977) (authentication established by "testimony from the officer who had taken the defendant's fingerprints that the proffered card was the one used in the fingerprinting"). In the case of business records, authentication can be established if a witness testifies that he is familiar with the business's record-keeping system and that the records in question "were made in good faith, kept in the normal course of business," made before the civil or criminal proceeding in which they are offered, and were relied on by the business's personnel. Commonwealth v. Driscoll, 91 Mass. App. Ct. 474, 480 (2017).

clear that there is no requirement that there be direct evidence to support a determination that a digital communication was sent by the defendant. Rather, a judge making this threshold determination may consider circumstantial evidence and look to "'confirming circumstances' sufficient for a reasonable jury to find by a preponderance of the evidence that the defendant authored the [electronic communication; here, the Facebook message containing the video]." Id. at 450, citing Commonwealth v. Hartford, 346 Mass. 482, 488 (1963).[20] Second, Purdy, supra, makes it clear that the mere possibility that a digital communication was fraudulently sent by someone other than the person associated with a particular social media or e-mail account from which the communication originated is not a bar to its authentication.[21] The principles set forth in Purdy are embodied in Mass. G. Evid. § 901(b)(11), and we have applied

[20] Direct or circumstantial evidence may authenticate proffered evidence. Such authenticating evidence may include the "appearance, contents, substance, internal patterns, or other distinctive characteristics of the item, taken together with all the circumstances." Mass. G. Evid. § 901(b)(4).

[21] See Purdy, 459 Mass. at 450, quoting United States v. Safavian, 435 F. Supp. 2d 36, 41 (D.D.C. 2006) ("The possibility of alteration does not and cannot be the basis for excluding e-mails as unidentified or unauthenticated as a matter of course, any more than it can be the rationale for excluding paper documents").

them in a number of decisions.[22] Third, in the absence of direct evidence, the common-law principles that have guided judges in determining, as a preliminary matter, whether written documents are authentic, see Mass. G. Evid. § 901(b)(4), are applicable to authentication issues in the context of digital communications. See Purdy, 459 Mass. at 448-450. See also United States v. Browne, 834 F.3d 403, 412 (3d Cir. 2016) ("[I]t is no less proper to consider a wide range of evidence for the authentication of social media records than it is for more traditional documentary evidence. The authentication of electronically stored information in general requires

---

[22] See, e.g., Gilman, 89 Mass. App. Ct. at 758-759 (sufficient confirming circumstances demonstrating that defendant authored Facebook messages attributed to him where account from which messages originated bore his name and picture, messages were downloaded from hard drives of two laptop computers issued to him by his employer and to which only he knew passwords, corroborating text messages initiating Facebook exchanges were sent from defendant's cell phone to victim's cell phone, and chats were "replete with personal references," including to events in which only defendant and victim participated and their nick names for each other); Oppenheim, 86 Mass. App. Ct. at 368 (sufficient confirming circumstances linking defendant to instant message communications included "familiar tone of the exchange," and defendant's reference in instant message to specific information from prior discussions with recipient); Commonwealth v. Amaral, 78 Mass. App. Ct. 671, 674-675 (2011) (e-mail communications properly authenticated by defendant's conforming behavior in waiting at specific time and place to meet undercover officer posing as underage prostitute and defendant's answering his cell phone when officer called). See also Connolly, 91 Mass. App. Ct. at 588 (requirement of authentication applied to testimony by police witness concerning contents of missing videotape).

consideration of the ways in which such data can be manipulated or corrupted, . . . and the authentication of social media evidence in particular presents some special challenges because of the great ease with which a social media account may be falsified or a legitimate account may be accessed by an imposter . . . . But the authentication rules do not lose their logical and legal force as a result"); Mass. G. Evid. § 901(a), (b)(4).

In response to the judge's request for an offer of proof concerning the authentication of the Facebook message to which the video was attached, the prosecutor informed the court that the message was received by the victim as a "Facebook message" on her cell phone as described above, that the victim had not seen or heard from the defendant during the past six or seven years, that the name on the account of the sender of the message was that of the defendant, "Urbano Meola," and that the video appeared to be self-authored. The judge also had been informed that the Facebook message included a photograph of the defendant's biological daughter (the victim's half-sister) and that several days after the victim received the offensive Facebook message, she received a "friend request" from the same account. The judge ruled that the video was admissible and that he would allow the victim to testify as to how she believed the video had come to her.

Although we have not found a Massachusetts case or a published opinion from another jurisdiction with facts exactly like those involved in this case, we conclude that the judge did not abuse his discretion in determining that the foundational facts constituted sufficient confirming circumstances to authenticate the Facebook message as having been sent by the defendant. First, we are mindful that the standard of review as to a judge's preliminary determination of authentication is deferential. See Leonard, 428 Mass. at 786 (prior bad act evidence). Moreover, by its nature, the judge's preliminary determination under Mass. G. Evid. § 104(b) is not conclusive and requires the finders of fact to make their own independent determination of the same question before they may consider the evidence. See Commonwealth v. Alden, 93 Mass. App. Ct. 438, 443 (2018) (trial judge instructed jury that "before they could consider the content of the text messages, the jury must be satisfied by a preponderance of the evidence that the messages had been sent by the defendant"). "Thus, after the proponent of the evidence has adduced sufficient evidence to support a finding that the proffered evidence is what it is claimed to be, the opposing party remains free to challenge the reliability of the evidence, to minimize its importance, or to argue alternative interpretations of its meaning, but these and similar other challenges go to the weight of the evidence -- not

to its admissibility" (quotation, citation, and emphasis omitted). United States v. Vayner, 769 F.3d 125, 131 (2d Cir. 2014). See Commonwealth v. Parrotta, 316 Mass. 307, 313 (1944).[23] Second, there is nothing in Purdy, the seminal Massachusetts decision on the authentication of digital evidence, or any other authoritative decision from Massachusetts or any other jurisdiction of which we are aware that precludes a judicial determination that digital evidence may be authenticated circumstantially based on its contents and the surrounding circumstances, even where, as here, there was no evidence of: a course of dealing between the defendant and the victim prior to the victim's receipt of a digital communication, account information supplied by the social media platform through which the message was sent, the Internet protocol (IP) address of the computer or device from which the message was sent,[24] or evidence that a copy of the message was found on a

[23] As noted earlier, the instant case was tried before a judge without a jury. The defendant did not file any requests for rulings of law. See Mass. R. Crim. P. 26, 378 Mass. 897 (1979). "A trial judge sitting without a jury is presumed, absent contrary indication, to have correctly instructed himself as to the manner in which evidence is to be considered in his role as factfinder." Commonwealth v. Batista, 53 Mass. App. Ct. 642, 648 (2002).

[24] "All computers that connect to the Internet identify each other through a unique string of numbers known as an . . . IP address. . . . In general, when a subscriber purchases Internet service from an Internet service provider (ISP), the ISP selects from a roster of IP addresses under its control and assigns a

device in the possession or under the control of the defendant.[25] Here, the judge not only had evidence that the Facebook message was from an account in the name of "Urbano Meola," but he also had evidence that the attached video depicted the "Urbano Meola" who is the defendant. And, the content of the attached video revealed highly intimate and personal details about the defendant that, because it was self-authored,[26] would be known only to the defendant or someone with whom he chose to share it. There was no evidence before the judge that the attached videotape had been shared with anyone else or otherwise published. Simply because evidence is digital or electronic in nature, as opposed to documentary, does not necessarily mean that it is widely available to others or to anyone other than its maker. Finally, the Facebook message also included a profile picture of the defendant's biological daughter. Again,

---

unique IP address to the subscriber at a particular physical address. . . . The IP address assigned to a particular subscriber may change over time, but the ISP keeps a log of which IP address is assigned to each subscriber at any given moment in time." Commonwealth v. Martinez, 476 Mass. 410, 410–411 (2017).

[25] See Parker v. State, 85 A.3d 682, 687-688 (Del. 2014). See also United States v. Sutton, 426 F.2d 1202, 1207 & n.37 (D.C. Cir. 1969), quoting 7 J. Wigmore, Evidence § 2148 (3d ed. 1940).

[26] As noted earlier, Detective Crowell described the video in question as having been taken "from down below, looking up towards the person in the video."

there was no evidence before the judge that this image had been published or was generally available to persons other than the defendant. And, the victim received a follow-up "friend request" from the same account a few days after she received the offensive videotape. Bearing in mind that "the possibility of alteration does not and cannot be the basis for excluding e-mails as unidentified or unauthenticated as a matter of course," Purdy, 459 Mass. at 450 (citation and emphasis omitted), we conclude that these "confirming circumstances" provided a basis for the judge's preliminary determination under Mass. G. Evid. § 104(b), that the Facebook message was an authentic communication from the defendant.[27] We reiterate, however, that in order to authenticate a digital communication such as a Facebook message, the proponent of the evidence must present "confirming circumstances" beyond simply the fact that the message was sent from an account in the name of the alleged author.[28]

---

[27] See generally Grimm, Cappa, & Joseph, Authenticating Digital Evidence, 69 Baylor L. Rev. 1, 11 (2017) ("It is a mistake for a judge to require the party introducing digital evidence to prove that no one other than the purported maker could have created the evidence if the introducing party has shown that, more likely than not, it was created by a particular person, unless there is evidence [not argument] that some other person could have done so").

[28] Cases illustrating deficiencies in the evidence offered to authenticate electronic communications include the following: Devbrow v. Gallegos, 735 F.3d 584, 586-587 (7th Cir. 2013)

4. Sufficiency of the evidence. When we review the denial of a motion for a required finding of not guilty, we ask "whether, after viewing the evidence in the light most favorable to the prosecution, any rational trier of fact could have found the essential elements of the crime beyond a reasonable doubt" (emphasis omitted). Commonwealth v. Latimore, 378 Mass. 671, 677 (1979), quoting Jackson v. Virginia, 443 U.S. 307, 318–319 (1979). A fact finder may draw inferences based on common experience, so long as the inferences are reasonable and possible, even though not necessary. See, e.g., Commonwealth v. Mazariego, 474 Mass. 42, 46 (2016). In assessing the sufficiency of the evidence, at least in cases where it is based in part on the testimony of witnesses, we also bear in mind that "[t]he weight . . . of the witnesses' testimony [is] solely for the fact finder and [is] not [a] proper subject[] for appeal"

(plaintiff failed to authenticate e-mail he allegedly received from defendant prison official where no circumstantial evidence presented indicating it was genuine); State v. Eleck, 130 Conn. App. 632, 641–642 (2011) (messages shown to have originated from Facebook account were not authenticated in circumstances in which account holder testified that her account had been hacked and content of messages did not bear any distinctive characteristics suggesting that they were sent by account holder); Smith v. State, 136 So. 3d 424, 434 (Miss. 2014) (authentication of Facebook messages not established by evidence that they originated from account in defendant's name and were accompanied by "small, grainy, low-quality photograph" that could not be determined to be that of defendant). See also United States v. Jackson, 208 F.3d 633, 638 (7th Cir. 2000).

(citation omitted). Commonwealth v. Lewis, 91 Mass. App. Ct. 651, 663 (2017).

In the present case, on the basis of the Facebook message from "Urbano Meola" to the victim, including a profile picture of the defendant's biological daughter (the victim's half-sister), accompanied by what could be found to be a self-authored video of the defendant, unclothed and touching his penis and anus, along with the evidence that the defendant, his biological daughter, the victim's mother, and the victim lived in the same household for six years, the judge, as the finder of fact, was warranted in concluding beyond a reasonable doubt that the defendant purposefully disseminated matter harmful to a minor to the victim, knowing that she was a minor, in violation of G. L. c. 272, § 28. See Commonwealth v. Mienkowski, 91 Mass. App. Ct. 668, 673 (2017). Accordingly, there was no error in denying the defendant's motion for a required finding.

Conclusion. For the above reasons, the Facebook message was sufficiently authenticated as having been sent to the victim by the defendant. The defendant's motion in limine seeking its exclusion from evidence was properly denied. The judge, as the finder of fact, was warranted in considering that the Facebook message was sent by the defendant. Taken as a whole, the evidence presented by the Commonwealth was sufficient to permit

the judge to conclude beyond a reasonable doubt that the defendant violated G. L. c. 272, § 28.

Judgment affirmed.