NOTICE: All slip opinions and orders are subject to formal revision and are superseded by the advance sheets and bound volumes of the Official Reports. If you find a typographical error or other formal error, please notify the Reporter of Decisions, Supreme Judicial Court, John Adams Courthouse, 1 Pemberton Square, Suite 2500, Boston, MA, 02108-1750; (617) 557-1030; SJCReporter@sjc.state.ma.us

25-P-347 Appeals Court
25-P-607

COMMONWEALTH vs. MICHAEL HAYES (and a companion case[1]).

Nos. 25-P-347 & 25-P-607.

Middlesex. October 3, 2025. - September 24, 2026.

Present: Rubin, Shin, & Singh, JJ.

Stalking. Intimidation of Witness. Witness, Intimidation. Protective Order. False Impersonation & Identity Fraud. Unauthorized Access to Computer System. Search and Seizure, Warrant, Computer. Cellular Telephone. Electronic Mail. Evidence, Photograph, Authentication. Practice, Criminal, Motion to suppress, Warrant, Required finding, Instructions to jury, Sentence.

Indictments found and returned in the Superior Court Department on February 5, 2021, and June 29, 2022.

A pretrial motion to suppress evidence was heard by Diane C. Freniere, J.; the cases were tried before William F. Bloomer, J.; a motion to revise or revoke sentence was heard by him; and a motion for reconsideration was considered by him.

Christopher DeMayo for the defendant.
Chia Chi Lee, Special Assistant District Attorney, for the Commonwealth.

---

[1] The companion case involves the same parties.

SINGH, J. Following a jury trial in the Superior Court where he represented himself, the defendant was convicted of stalking, witness intimidation, violation of a harassment prevention order, criminal harassment, identity fraud, attempted identity fraud, and unauthorized access to a computer system. On appeal, the defendant challenges the denial of a motion to suppress evidence seized from his cell phone, the sufficiency of the evidence on a charge of witness intimidation, the correctness of jury instructions concerning authentication of electronic communications, and the propriety of factors considered in sentencing. The Commonwealth appeals from the reduction in the defendant's sentence two years after initial sentencing and from the denial of its motion to reconsider the sentence reduction. We affirm the judgments, the order reducing the sentence, and the order denying the motion to reconsider the reduction in sentence.[2]

Background. The defendant met the victim in 2005, when the two were in a class together during their junior year of high school. He asked her on a date, but she declined. To be kind, the victim told the defendant they could be friends and gave him her telephone number. The defendant started calling the victim, asking her to hang out and telling her he loved her. She became

[2] We have paired these two appeals for consideration by the same panel.

uncomfortable and told him she only wanted to be friends in school. At school, the defendant waited for the victim outside of her classes and followed her around. When the victim asked him to leave her alone, he yelled and swore at her to the point that others had to intervene. The victim's mother had a meeting with school officials, as well as the defendant and his parents, in which the defendant was told to leave the victim alone. He did not.

The defendant kept contacting the victim through notes and e-mail messages. The e-mail messages started off friendly and apologetic, with the defendant writing that he tried to leave the victim alone, was not a bad person, and would leave her alone if she answered him. She never did.

The victim went to college the following year, and she started receiving e-mail messages from the defendant at her college e-mail address. When the victim did not respond, the e-mail messages escalated in tone, using profanity and becoming sarcastic, angry, and threatening. After the victim blocked the defendant from her social media accounts, the defendant implored her to unblock him, at times implying that he would do something negative to her and at other times hinting that he would hurt himself.

In 2009, when the victim returned from a study abroad program, she found her car to have been "keyed all over the entire thing from top to bottom." She reported this to the police and obtained a harassment prevention order against the defendant; he was ordered to stay away from her.[3] A couple years later, however, the defendant twice approached the victim at a gym. The victim ended her membership, fearing that the defendant would keep approaching her. Because an earlier stay away order was still in place, the defendant was again told to stay away from the victim.

In December 2015, the defendant suffered a stroke. While in the hospital, he sent the victim an e-mail message, this time to her work e-mail. In the e-mail message, the defendant said that he was not going to stalk the victim but that he would always love her. The victim contacted the police and obtained a one-year harassment prevention order against the defendant, which required him to have no contact with her, direct or indirect.

While the one-year order was still in place, however, the victim received a series of e-mail messages, apparently from the defendant, through various anonymous addresses. In these e-mail messages, the defendant threatened to end his life, blamed the victim and her family for his situation, referred to the harassment prevention order as the victim's family's way of

---

[3] The defendant implied to a friend that he was responsible for keying the victim's car.

punishing him, and said he wanted the order lifted so that they could start over again. The defendant also contacted the victim's mother through Facebook and told her that the harassment prevention order was ruining his career prospects (he wanted to go into law enforcement). He said that it would be in everyone's best interest to lift the order or else he would make them come back every year to renew it. In December 2016, the victim sought and obtained a permanent harassment prevention order.

Thereafter, the victim began receiving alerts about login attempts to all her social media accounts. Subsequently, in March 2019, the victim received a text message from a stranger, saying that someone had tried to hire that person to hack into the victim's Facebook and Google accounts.[4] The victim reported

---

[4] The stranger, a self-described "hacker," explained that the term originally referred to people who could "hack together something . . . a quick and dirty solution." People "would call themselves hackers if they were able to write code that was particularly clever and useful." The term later evolved to become synonymous "at least [in] the popular culture with computer crime, even though that's not what hacking means." According to the hacker, the defendant had reached out through a "Discord server" (described by the hacker as a forum or chat room) comprised of cyber security enthusiasts and asked about getting into the victim's accounts. Concerned about the defendant's intentions, the hacker tried to discover the defendant's identity to turn the information over to the police. Later, the hacker became one of the defendant's witness intimidation victims.

this information to the police, who began investigating the matter.

In November 2019, the victim received a series of five unanswered telephone calls in quick succession from numbers that were not in her contacts -- she recognized the last number as being connected to the defendant. She reported the calls to the police, who obtained an arrest warrant for the defendant and a search warrant for his electronic devices.[5] Following execution of the search warrant, the defendant was charged with violating the harassment prevention order.

While that charge was pending, the victim continued to receive alerts about login attempts to her accounts, as well as text messages and e-mail messages from unknown senders. One of the e-mail messages, apparently from the defendant, said that he had succeeded in what he was attempting to do, and that if the victim did not stop going forward with the trial, he would embarrass her. The victim's mother also received an e-mail

[5] Among the items recovered from execution of the 2019 search warrant for the defendant's electronic devices were screenshots of login pages on accounts belonging to others, including the victim, as well as screenshots of conversations with the hacker. There were entries in the Notes application titled "Hacking Facebook profiles" and "Hacking Snapchats." Within a pictures folder, there was a folder with the victim's name and another that contained images of someone of the victim's likeness -- a photograph that had been altered to make her appear partially nude.

message from an unknown sender saying, "So you won't mind if I get your daughter arrested for possession of child pornography . . . and ruin her teaching career . . . ."

In August 2020, the victim's mother received a series of e-mail messages from e-mail addresses that appeared to belong to different women.[6] The e-mail messages said,

> "If I spend one day behind bars, I'll hunt your husband down.
>
> "I'll put your husband in the ground. I dare you to give me a dirty look or ruin my life more than you did. Instigate me some more. See what happens.
>
> "And if you ever give me a dirty look, I'll kill you and your husband.
>
> "Tell your husband, if he ever tries to get me fired at a job, I'll cut his head off while he's still alive."

The victim's family reported these e-mail messages to the police, and in 2020, the police obtained another arrest warrant for the defendant and a search warrant for additional electronic devices.[7] After this arrest, the defendant remained in custody,

---

[6] The e-mail messages were sent from the accounts of four different women, each of whom testified at trial that they did not know the defendant and that they did not send the e-mail messages in question; each of them also had private Snapchat photographs that had been compromised. These women were victims of the defendant's identity fraud and unauthorized access to computer systems.

[7] Execution of the 2020 search warrant for the defendant's electronic devices revealed, among other things, evidence of calls corresponding with the series of five missed calls to the victim and e-mail account information of different women corresponding with those used to threaten the victim's family.

and the threats to the victim's family from unknown e-mail addresses ceased.

Discussion. 1. Motion to suppress. The defendant claims that the motion judge erred in denying his motion to suppress evidence obtained from the 2019 and 2020 searches of his electronic devices. On appeal, he does not dispute that the warrants were supported by probable cause. Rather, he contends that the police exceeded the scope of the 2019 search authorized by warrant, and then used that unlawfully obtained evidence to secure the 2020 search warrant. He argues that images (photographs and screenshots) and files from the phone's "Notes" application seized during the 2019 search should have been suppressed as beyond the scope of the warrant and all evidence from the 2020 search warrant should have been suppressed as fruits of the unlawful 2019 search.

In our review of the denial of a motion to suppress evidence, we accept the judge's subsidiary findings of fact, absent clear error, and independently review the ultimate findings and conclusions of law. See Commonwealth v. Barillas, 484 Mass. 250, 253 (2020). Where the search was conducted pursuant to a warrant, the defendant bears the burden of establishing that evidence was illegally obtained. See

Commonwealth v. _Carleton_, 497 Mass. 11, 29 (2026), citing _Commonwealth_ v. _Taylor_, 383 Mass. 272, 280 (1981). The defendant also bears the burden when the claim is that the search exceeded the scope of the warrant. See _Carleton_, _supra_, citing _Taylor_, _supra_.

Here, the 2019 warrant authorized the police to search for and seize from the defendant's electronic devices:

> "a) Internet Search History relating to communication or attempted communication with [the victim or her mother]
>
> "b) Communication History be it Internet chat history, e-mail, text message, phone call logs etc. Including contact lists, relating to communication or attempted communication with [the victim or her mother]
>
> "c) Login history for both email and social media applications
>
> "d) Data related to the creation use or purchase of, password manipulation software, virus, malware, and related software that could be utilized to infiltrate or compromise the e-mail and/or social media accounts of [the victim]."

The defendant contends that this authorization, by its terms, did not include images (screenshots and photographs) or the Notes application.

A search of electronic devices, however, "may be as extensive as _reasonably_ required to locate the items described in the warrant" (citation omitted). _Commonwealth_ v. _Dorelas_, 473 Mass. 496, 502 (2016). Where the warrant did not specify particular files or applications to be searched, the police were justified in searching any files or applications that could reasonably contain the specified evidence. See Commonwealth v. Henley, 488 Mass. 95, 119-120 (2021) (where police could not know precise location within cell phone where evidence would be found, they were justified in searching for particularized evidence in areas where it would be reasonable to look for it).

Here, the warrant did not specify that screenshots could be seized, but it did authorize the seizure of "[l]ogin history," which would encompass the screenshots of login pages of accounts belonging to others including the victim. It also authorized the seizure of "[c]ommunication [h]istory" and "[d]ata related to . . . password manipulation . . . and related software that could be utilized to infiltrate or compromise . . . accounts of [the victim]." This would encompass the screenshots of conversations with the hacker related to accessing the victim's accounts. And although the warrant did not specify that photographs could be seized, the police reasonably opened a picture folder when they came across one with the victim's name on it, as it reasonably contained "communication history," specifically relating to communications or attempted communications with the victim. See Dorelas, 473 Mass. at 497 ("where there was probable cause that evidence of communications relating to and linking the defendant to the crimes under investigation would be found in the electronic files on the iPhone, and because such communications can be conveyed or stored in photographic form, a search of the photograph files was reasonable"). Likewise, the Notes application was a reasonable place to search for evidence of the defendant's own notations regarding attempts to communicate with the victim and her mother, as well as his attempts to infiltrate their accounts. Moreover, the Notes entries entitled "Hacking Facebook profiles" and "Hacking Snapchat" fell squarely within the category of data related to infiltrating the victim's accounts.

The judge properly denied the defendant's motion to suppress as the search and seizure did not exceed the scope of the warrant.

2. Required finding of not guilty as to witness intimidation. The defendant next claims that the judge erred in denying his motion for a required finding of not guilty on the witness intimidation charge relating to a mailing sent to the hacker while the defendant was in jail awaiting trial in this matter. To withstand a motion for a required finding of not guilty of witness intimidation, the Commonwealth was required to present evidence from which the jury could find beyond a reasonable doubt that the defendant (1) willfully (2) threatened, intimidated, or harassed (3) a witness in a criminal proceeding of any type (4) with intent to impede or interfere with a criminal investigation or proceeding. See

Commonwealth v. Gardner, 102 Mass. App. Ct. 299, 304 (2023). On appeal, the defendant challenges only the sufficiency of the evidence that he "threatened, intimidated or harassed," id., the hacker. The defendant's claim is that the witness intimidation statute, G. L. c. 268, § 13B, punishes only constitutionally unprotected speech, and that therefore, he could not be convicted unless the mailing constituted a "true threat" against the hacker. Although we agree that the statute may not punish constitutionally protected speech, we disagree that the defendant's conduct toward the hacker was protected by the First Amendment to the United States Constitution. See Commonwealth v. Johnson, 470 Mass. 300, 309 (2014) (First Amendment does not provide defense to criminal conduct simply because defendant uses words to carry out illegal purpose).

We briefly summarize the pertinent evidence in the light most favorable to the Commonwealth. See Commonwealth v. Latimore, 378 Mass. 671, 676-677 (1979). In March 2021, while the defendant remained in custody, he sent to the hacker in the mail what appeared to be a printout of the hacker's driver's license information, including date of birth and residential address. The printout had a photograph of the hacker's face with a swastika drawn on the forehead. In addition, a variety of accusations, insults and slurs (incorporating the names of people involved in the prosecution against the defendant) were handwritten across the page.[8]

From the references to persons involved in the prosecution and the anger reflected in the comments, the jury could have found that the defendant was targeting the hacker based on his awareness that the hacker had played a role in launching the investigation that landed the defendant in jail. The jury also could have found that the hacker's interactions with the defendant through Discord, see note 4, supra, left the hacker aware of the defendant's obsessive nature. Moreover, the jury could have found that the mailing itself was intended to intimidate the hacker by demonstrating the defendant's ability to access the hacker's personal information, to get a personal mailing to his home, and to do so while in custody.[9]

As to whether the content of the mailing constituted a true threat, it is to be "measured objectively, considering whether,

---

[8] The handwritten notations were: "FBI Faggot," "GOVERNMENT CRIMINAL SCUM," "Wilson Street Worcester," "Best friends with Middlesex ADA [name]," "Butt buddy of Det[. name] another fag," and "WANTED FOR IDENTITY FRAUD, OBSTRUCTION OF JUSTICE, providing a false name to a police officer, and for being a Ginger with a terrible combover." As reflected in his cross-examinations at trial, the defendant had a theory that the hacker was a "Deep State" operative, meaning "corrupt elements in the FBI and DOJ," working to ensnare him.

[9] The return address on the mailing plainly identified the defendant as an "inmate" with the address of the jail at which the defendant was being held.

in light of the attendant circumstances, the words justifiably caused the recipient to fear violence."[10] Commonwealth v. Cruz, 495 Mass. 110, 113 (2024). See Commonwealth v. Chou, 433 Mass. 229, 236 (2001) (term "true threat" distinguishes between "words that literally threaten but have an expressive purpose such as political hyperbole, and words that are intended to place the target of the threat in fear, whether the threat is veiled or explicit"). Against this evidentiary backdrop, the photograph of the hacker with a hand-drawn swastika on the forehead, sent to the hacker by the defendant, who remained in jail as a result of the hacker's betrayal, could have been found by the jury to amount to a threat that objectively justified the hacker in fearing violence. We are satisfied that the mailing constituted a true threat, not protected by the First Amendment, and that the trial judge properly denied the defendant's motion for a required finding. See Cruz, 495 Mass. at 113 (true threat is serious expression of speaker's intent to commit act of unlawful violence).

---

[10] Although the communication is evaluated objectively to determine whether it constitutes a true threat, the Commonwealth must also show that the defendant was at least aware that others could regard his statements as threatening violence and delivered them anyway. Cruz, 495 Mass. at 113, citing Counterman v. Colorado, 600 U.S. 66, 69, 79 (2023) (mens rea required for delivering true threat must be recklessness at minimum). This element of the charge is not at issue in this appeal.

3. Jury instructions. The defendant claims that the judge erred in giving, over his objection, a jury instruction on authentication of electronic communications that allegedly confused the jury and impermissibly lowered the Commonwealth's burden of proof. Specifically, he contends that "authorship [of] the electronic communications was an element of virtually all charges and therefore had to be proved beyond a reasonable doubt," so "[t]here was no need to instruct the jurors to first determine under a preponderance standard whether [the defendant] had authored the communications before making that very same determination under a reasonable doubt standard." He also claims that the judge erred in rejecting his proposed instruction that the jurors had to find that he authored the communications beyond a reasonable doubt. We review an alleged jury instruction error to which the defendant objected for prejudicial error. Commonwealth v. Cruz, 445 Mass. 589, 591 (2005).

The judge addressed authentication of electronic communications at several points during trial -- at the time of admission of the evidence, in final instructions, and in response to jury questions. Each time, the judge correctly instructed that, to consider an electronic communication, there must be a preliminary determination, by a preponderance of the evidence, that the defendant in fact authored the communication.

See Commonwealth v. Purdy, 459 Mass. 442, 447 (2011). During final instructions and in response to jury questions, the judge correctly followed up with an instruction that the Commonwealth had the burden to prove each element of the crimes charged beyond a reasonable doubt. See id. There was no error in these instructions.

Contrary to the defendant's argument, the authentication instruction was not superfluous. As authentication is preliminary to relevance, a determination must first be made that an electronic communication is what it purports to be, that is, a communication authored by the defendant, in order to be relevant to the issues at trial. See Commonwealth v. Meola, 95 Mass. App. Ct. 303, 307-308 (2019) (authentication is condition precedent to admissibility of electronic communication). The judge initially determines "whether there is evidence sufficient, if believed, to convince the jury by a preponderance of the evidence that the item in question is what the proponent claims it to be" (citation omitted). Purdy, 459 Mass. at 447. The judge's preliminary determination as to admissibility, however, is not conclusive; even after the evidence is admitted, "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" (citation omitted). Meola, supra at 313. Thus, the jury must still make their own independent determination, by a preponderance of the evidence, that the defendant authored the communication before considering the evidence. See id., citing Commonwealth v. Alden, 93 Mass. App. Ct. 438, 443 (2018).

The judge also correctly instructed the jury about the burdens of proof applicable to authentication and the elements of the offense, respectively. Whether the defendant authored the communications was a question preliminary to the jury's inquiry on the elements of the crime and needed only to be proven by a preponderance of the evidence. See Commonwealth v. Oppenheim, 86 Mass. App. Ct. 359, 366-367 (2014) (preliminary questions of fact need only be proven by preponderance, no matter how closely associated with elements of crime required to be proven beyond reasonable doubt). From there, and regardless of the jury's determination on authentication, they must go on to consider whether the Commonwealth proved each element of the crimes charged beyond a reasonable doubt.

Pointing to jury questions, the defendant argues that the authentication instructions, in the circumstances of this case, served only to confuse. The somewhat subtle distinction between authorship of the electronic communications as it relates to authentication versus guilt, particularly with respect to the charges at issue in this case, understandably gave rise to jury questions.[11] See Alden, 93 Mass. App. Ct. at 444 ("We acknowledge that in this case there was a fine line between the (1) preliminary determination of the authenticity of the text messages and (2) proof of the defendant's identity as the perpetrator of the threats. Nevertheless, authenticity and identity are different legal concepts").

The judge answered the jury questions by correctly instructing that the jurors had to "determine whether [they] believe that it is more likely true than not true" that the defendant authored the e-mail messages before considering the content of the e-mail messages. He went on to explain that, if they could not find by a preponderance that the defendant authored the e-mail messages, they were to disregard those e-mail messages and make their determination based on the remaining evidence. He reiterated that "the burden is always on the government to prove the charge beyond a reasonable doubt,

[11] The jury asked, "With respect to indictments six through nine [violation of harassment prevention order], in relation to point number three, do we need a preponderance of the evidence to determine the author of the emails, or do we need to be beyond a reasonable doubt that the defendant authored the emails?" Additionally, the jury asked, "We've read the electronic communication sections [of the jury instructions] and are unclear if that supersedes the language beyond a reasonable doubt as stated in paragraph one of indictments six through nine."

not by a preponderance of the evidence" and emphasized that the jurors had to determine whether the government had proven each of the elements of the crime beyond a reasonable doubt.

These are accurate instructions and we must presume the jury followed them, not speculate that the jurors may have remained confused.[12] See Commonwealth v. Andre, 484 Mass. 403, 418 (2020) (properly instructed jury presumed to understand and follow law). See also Commonwealth v. Middleton, 100 Mass. App. Ct. 756, 757-760 (2022) (affirming convictions of stalking in violation of restraining order, violation of G. L. c. 209A order, and witness intimidation where judge gave preponderance instruction on authentication three times and made clear that Commonwealth bore burden to prove beyond reasonable doubt that defendant committed each offense).

A review of the instructions as a whole shows that the judge repeatedly accurately instructed on authentication and emphasized that the Commonwealth must prove the elements of each offense beyond a reasonable doubt. See Commonwealth v. Glacken, 451 Mass. 163, 168-169 (2008) (in reviewing instructions to

---

[12] We do not reach the question whether it would have been in the judge's discretion, if agreed to by both parties, to give no authentication instruction at all, but instead to make the preliminary determination as to the authentication of the evidence, leave it to the parties to argue the weight of the evidence, and then instruct on the elements of the crime.

jury, phrases are not to be taken in isolation, but rather instructions to be evaluated as whole for interpretation reasonable jurors would place on judge's words). Accordingly, we conclude that the authentication instruction was not erroneous and did not lower the burden of proof. Further, the judge did not err in giving the instruction, nor in rejecting the defendant's proposed instruction.

4. Sentencing. Both parties raise issues regarding sentencing. The defendant challenges the propriety of factors considered in his initial sentencing. The Commonwealth appeals from the judge's reduction in the defendant's sentence almost two years later and the denial of its motion to reconsider the reduction in sentence. Because we affirm the reduction in sentence, the defendant's claims regarding the initial sentencing are moot and we do not address them.[13]

After his initial sentencing immediately following trial, the defendant timely moved to revise or revoke his sentence; that motion was denied. In the next several months, the defendant continued to send correspondence to the court and to make additional filings, including motions to reconsider earlier rulings and additional motions to revise or revoke. The judge

[13] This is consistent with the defendant's position on appeal, as he has stated he is satisfied with the revised, reduced sentence.

treated the series of filings as a motion to reconsider the denial of the motion to revise or revoke.[14] He requested the probation department to do a Brief Risk Assessment for Violent Offending (BRAVO) report with the defendant through a program that did not exist when the defendant was first sentenced. The report was made available to the parties. After a hearing, the judge reduced the incarcerated portion of the defendant's sentence and revised the terms of his probation. The judge denied the Commonwealth's timely motion for reconsideration of the sentence revision.

On appeal, the Commonwealth contends that the judge erred in improperly considering a fact that did not exist at the time of sentencing, specifically, the BRAVO report. We review the propriety of a reduction in sentence on a motion to revise or

[14] The Commonwealth maintains that the defendant's motion for reconsideration should be considered untimely because it was not filed within thirty days of the denial of the motion to revise or revoke. See Mass. R. Crim. P. 29 (a) (1), as appearing in 489 Mass. 1503 (2022). The defendant did file a motion within thirty days, but it was labeled a motion for a new trial. Although the motion did not explicitly seek reconsideration of sentencing, it did complain about prosecutors requesting an upward departure from sentencing guidelines. In these unique circumstances, it was within the judge's discretion to treat that motion, in conjunction with all of the subsequent motions, as a timely request to reconsider the denial of the defendant's motion to revise or revoke. See Commonwealth v. Curtis, 53 Mass. App. Ct. 636, 637-639 (2002) (cautioning against considering form over substance when reviewing timeliness of motions).

revoke for an abuse of discretion. See Commonwealth v. Malick, 86 Mass. App. Ct. 174, 185 (2014). It is well established that on a motion to revise or revoke, a judge may not take into account conduct of the defendant that occurs subsequent to the original sentencing. See Commonwealth v. DeJesus, 440 Mass. 147, 152 (2003). Use of postconviction conduct to alter a sentence could intrude on the purview of the executive branch. See Commonwealth v. McGuinness, 421 Mass. 472, 476 n.4 (1995) (defendant's actions postsentencing best left to parole board).

Although the judge here did consider the newly produced BRAVO report, it is apparent from the record that he did not consider postconviction conduct of the defendant. Cf. Commonwealth v. Tejeda, 481 Mass. 794, 795-797 (2019) (recognizing that cases emphasizing the prohibiting of consideration of postconviction evidence have focused on defendant's conduct or denial of parole). Rather, he used an additional tool to analyze the information available at the time of sentencing. The judge explicitly noted that he did not reconsider and revise the sentence based on any of the defendant's postconviction rehabilitation efforts. And there is nothing in the record to suggest otherwise.

The judge explained that he had grappled with the issue of sentencing in this particular case and sought a newly available probation tool to provide guidance in considering "the alternatives available to achieve the goals of sentencing: protecting the public, providing just punishment to the defendant, deterring future criminal conduct, and rehabilitating [the defendant]." See Commonwealth v. White, 436 Mass. 340, 343 (2002) (discussing punishment, deterrence, protection of public, and rehabilitation as appropriate goals of sentencing). In other words, he sought to impose a more "just" sentence. See DeJesus, 440 Mass. at 152 (purpose of motion to revise or revoke is to permit judge to reconsider sentence imposed and determine whether sentence was just). We therefore find no cause to disturb the reduction of sentence.

Conclusion. The judgments are affirmed. The order revising the sentence is affirmed. The order denying the motion for reconsideration of the order revising the sentence is affirmed.

So ordered.