PRECEDENTIAL

UNITED STATES COURT OF APPEALS
FOR THE THIRD CIRCUIT

No. 14-1798

UNITED STATES OF AMERICA

v.

TONY JEFFERSON BROWNE,

Appellant

On Appeal from the District Court
of the Virgin Islands
(D.C. No. 3-13-cr-00037-001)
District Judge: Curtis V. Gomez

Argued December 10, 2015

BEFORE: FISHER, KRAUSE, and ROTH, *Circuit Judges*

(Filed: August 25, 2016)

Everard E. Potter, Esq. [ARGUED]
Ronald Sharpe, Esq.
Office of United States Attorney
5500 Veterans Building, Suite 260
United States Courthouse
St. Thomas, VI 00802

Counsel for Appellee

Omodare Jupiter, Esq. [ARGUED]
Office of Federal Public Defender
1115 Strand Street
Suite 201
Christiansted, VI 00820

Counsel for Appellant

OPINION OF THE COURT

Krause, *Circuit Judge*.

The advent of social media has presented the courts with new challenges in the prosecution of criminal offenses, including in the way data is authenticated under the Federal Rules of Evidence—a prerequisite to admissibility at trial. Appellant Tony Jefferson Browne was convicted of child pornography and sexual offenses with minors based in part on records of "chats" exchanged over Facebook and now contests his conviction on the ground that these records were not properly authenticated with evidence of his authorship. Although we disagree with the Government's assertion that,

pursuant to Rule 902(11), the contents of these communications were "self-authenticating" as business records accompanied by a certificate from the website's records custodian, we will nonetheless affirm because the trial record reflects more than sufficient extrinsic evidence to link Browne to the chats and thereby satisfy the Government's authentication burden under a conventional Rule 901 analysis.

I. Background

A. Facts

Facebook is a social networking website that requires users to provide a name and email address to establish an account. Account holders can, among other things, add other users to their "friends" list and communicate with them through Facebook chats, or messages.

Under the Facebook account name "Billy Button," Browne began exchanging messages with 18-year-old Nicole Dalmida in November 2011. They met in person a few months later and then exchanged sexually explicit photographs of themselves through Facebook chats. Browne then threatened to publish Dalmida's photos online unless Dalmida engaged in oral sex and promised to delete the photos only if she provided him the password to her Facebook account.

Using Dalmida's account, Browne made contact with four of Dalmida's "Facebook friends," all minors—T.P. (12 years old), A.M. (15 years old), J.B. (15 years old) and J.S. (17 years old)—and solicited explicit photos from them by a variety of means. Once he had the minors' photos, he

repeated the pattern he had established with Dalmida, threatening all of them with the public exposure of their images unless they agreed to engage in various sexual acts and sent additional explicit photos of themselves to his Button Facebook account or to his phone number ("the 998 number"). He arranged to meet with three of the minors and sexually assaulted one.

On receiving information from the Virgin Islands Police Department, agents from the Department of Homeland Security (DHS) interviewed Dalmida and three of the minors. In June 2013, DHS arrested Browne and executed a search warrant on his residence. Among the items seized was a cell phone that matched the 998 number and from which text messages and photos of the minors were recovered. During questioning and at trial, Browne admitted the 998 number and phone belonged to him. DHS executed a search warrant on the Button Facebook account, which Browne also admitted belonged to him, and Facebook provided five sets of chats and a certificate of authenticity executed by its records custodian.

B. Proceedings

At trial, over defense counsel's objections, the District Court admitted the five Facebook chat logs and certificate of authenticity into evidence. Four of the chats involved communications between the Billy Button account and, respectively, Dalmida, J.B., J.S. and T.P. [1] The fifth chat did

[1] The Government did not seek to admit into evidence any Facebook messages sent from the Button account to the remaining minor victim, A.M., but photos of A.M. were

not involve Button's account and took place between Dalmida and J.B., on the subject of Browne's sexual assault of J.B. The certificate stated, in accordance with Rule 902(11) of the Federal Rules of Evidence, that the records that Facebook had produced for the named accounts met the business records requirements of Rule 803(6)(A)–(C). Tracking the language of Rule 803(6), the custodian certified that the records "were made and kept by the automated systems of Facebook in the course of regularly conducted activity as a regular practice of Facebook . . . [and] were made at or near the time the information was transmitted by the Facebook user." App. 403; *see* Fed. R. Evid. 803(6).

Relevant to this appeal, seven witnesses testified for the Government: Dalmida and the four minors, and two Special Agents from DHS. Dalmida and the four minors provided extensive testimony about their communications with Button. According to that testimony, using Dalmida's Facebook account, Browne sent explicit photos of Dalmida to T.P. and A.M. and requested photos in return, and using his own Facebook account, he contacted J.S. and offered to pay her for sexually explicit photos of herself. The testimony and chat logs also established that Browne used Dalmida's account to instruct J.B. to add him as a friend on Facebook, after which he used his own account to send her explicit photos of himself and asked her to do the same.

All four minors testified that after receiving requests for explicit photos, they complied by sending Facebook messages to the Button account or by texting images to the

---

among those recovered from the phone seized from Browne's home and admitted into evidence.

998 number, and that they subsequently received threats that their photos would be published online if they did not comply with the sender's sexual demands. And on the stand, Dalmida and each of the four minors identified various Government exhibits as photos they took of themselves and sent to the Button account or the 998 number.

Dalmida and three of the minors (all but T.P.) also testified to meeting Browne in person and identified Browne in open court as the man they had met after making meeting arrangements through messages to the Button account or the 998 number. Two of the minors who met Browne in person testified that they were forced to do more than send additional explicit photographs. A.M. explained that after receiving instructions to text her photos to the 998 number, she received messages from the Button account demanding sexual intercourse and threatening her with the exposure of her images if she refused. After sending her the images, presumably to prove they were in his possession, the individual using the 998 number repeated his threat and instructed her to "play with [her]self" on a video chat site so he could watch. Fearful he would follow through on his threat, she complied. Another minor, J.B., testified that after she arranged to meet Browne through the Button account, Browne sexually assaulted her and recorded the encounter. She also confirmed that she exchanged Facebook messages with Dalmida describing the incident shortly after it occurred.

Special Agents Blyden and Carter testified to details of Browne's arrest and the forensics examination of the items seized from Browne's residence. Special Agent Blyden recounted Browne's post-arrest statements that he knew and had exchanged "nude photos" with Dalmida, that he admitted to knowing three of the minors (all but A.M.), and that he had

paid minor J.S. for nude photos of herself. Special Agent Blyden also identified the Facebook chat conversations as records she had received from Facebook and testified that Facebook had provided the accompanying certificate. Special Agent Carter, the forensics agent, testified to the items recovered from Browne's home, including the phone associated with the 998 number, and identified sexually explicit photos of Dalmida and three of the minors (all but J.B.) as images that were recovered from the phone.[2]

The defense put only Browne on the stand. Browne testified that his Facebook name was Billy Button, and that he knew Dalmida and minors J.S. and J.B. and had corresponded with them on Facebook. He denied knowing or communicating with minor T.P., contradicting Special Agent Blyden's testimony that he had admitted to this after his arrest, and did not state whether he knew A.M. Browne also denied sending any photos to the victims or requesting photos from them. As to the incriminating data discovered on the phone with the 998 number, he testified that he loaned the phone to Dalmida in December of 2012 and intermittently between January and March 2013, and that he also loaned the phone to a cousin at an unspecified time.[3] At one point

[2] At trial, however, J.B. identified several Government exhibits as photos she had sent to Button's Facebook account or the 998 number.

[3] Dalmida testified that she never had Browne's phone in her possession, and Special Agent Blyden testified that during the investigation Dalmida denied ever receiving a phone from Browne.

during his testimony, he confirmed he owned a second phone and number ("the 344 number").

Browne was convicted by a jury after a two-day trial.[4] He now appeals his conviction on the ground that the Facebook records were not properly authenticated and should not have been admitted into evidence.

II. Jurisdiction

[4] The jury convicted Browne on twelve counts, including the production of child pornography in violation of 18 U.S.C. § 2251(a) (Counts 1–4); the coercion and enticement of a minor to engage in sexual activity in violation of 18 U.S.C. § 2422(b) (Count 8); the receipt of child pornography in violation of 18 U.S.C. § 2252(a)(2) (Counts 9–12); and the transfer of obscene material to minors under age 16, in violation of 18 U.S.C. § 1470 (Count 17, 19–20). The jury acquitted Browne on three counts for coercion and enticement, in violation of 18 U.S.C. § 2422(b) (Counts 5–7), and on the count of aggravated first degree rape in violation of 14 V.I.C. § 1700(c) (Count 22). Before the jury rendered its verdict, the defense successfully moved to dismiss a charge of extortion using interstate commerce, in violation of 18 U.S.C. 875(d) (Count 21), and the Government successfully moved to dismiss one of the counts for the transfer of obscene material to minors under age 16 (Count 18) and all charges for possession of child pornography under 18 U.S.C. 2252(a)(4)(B) (Counts 13–16) in light of the fact that possessing child pornography is a lesser-included offense of the receipt of child pornography, *United States v. Miller*, 527 F.3d 54, 71–72 (3d Cir. 2008).

The District Court had jurisdiction under 18 U.S.C. § 3231 and 48 U.S.C. § 1612(c), and we have jurisdiction under 28 U.S.C. § 1291. We review the District Court's decision regarding the authentication of evidence for abuse of discretion, *United States v. Turner*, 718 F.3d 226, 232 (3d Cir. 2013), and exercise plenary review over its interpretation of the Federal Rules of Evidence, *United States v. Console*, 13 F.3d 641, 656 (3d Cir. 1993).

III. Discussion

Browne argues that the Facebook records were not properly authenticated because the Government failed to establish that he was the person who authored the communications. More specifically, Browne contends that no witness identified the Facebook chat logs on the stand; nothing in the contents of the messages was uniquely known to Browne; and Browne was not the only individual with access to the Button account or the 998 number. The Government, for its part, argues the Facebook records are business records that were properly authenticated pursuant to Rule 902(11) of the Federal Rules of Evidence by way of a certificate from Facebook's records custodian.

The proper authentication of social media records is an issue of first impression in this Court. In view of Browne's challenge to the authentication and admissibility of the chat logs, our analysis proceeds in three steps. First, as with non-digital records, we assess whether the communications at issue are, in their entirety, business records that may be "self-authenticated" by way of a certificate from a records custodian under Rule 902(11) of the Federal Rules of Evidence. Second, because we conclude that they are not, we consider whether the Government nonetheless provided

sufficient extrinsic evidence to authenticate the records under a traditional Rule 901 analysis. And, finally, we address whether the chat logs, although properly authenticated, should have been excluded as inadmissible hearsay, as well as whether their admission was harmless.

A. Self-authentication

To satisfy the requirement under Rule 901(a) of the Federal Rules of Evidence that all evidence be authenticated or identified prior to admission, the proponent of the evidence must offer "evidence sufficient to support a finding that the item is what the proponent claims it is." Rule 901(b), in turn, sets forth a non-exhaustive list of appropriate methods of authentication, including not only "[t]estimony that an item is what it is claimed to be," Fed. R. Evid. 901(b)(1), but also "appearance, contents, substance, internal patterns, or other distinctive characteristics of the item, taken together with all the circumstances," Fed. R. Evid. 901(b)(4), and "[e]vidence describing a process or system and showing that it produces an accurate result," Fed. R. Evid. 901(b)(9).

The central dispute in this case is complicated, however, by the Government's contention that it authenticated the Facebook chat logs by way of Rule 902, under which extrinsic evidence is not required for certain documents that bear sufficient indicia of reliability as to be "self-authenticating." Specifically, the Government relies on Rule 902(11), which provides that "records of a regularly conducted activity" that fall into the hearsay exception under Rule 803(6)—more commonly known as the "business records exception"—may be authenticated by way of a certificate from the records custodian, as long as the proponent of the evidence gives the adverse party reasonable

notice and makes the record and certificate available for inspection in advance of trial. Fed. R. Evid. 902(11).[5]

The viability of the Government's position turns on whether Facebook chat logs are the kinds of documents that are properly understood as records of a regularly conducted activity under Rule 803(6), such that they qualify for self-authentication under Rule 902(11). We conclude that they

[5] Rule 803(6) allows for the admission of "[a] record of an act, event, condition, opinion, or diagnosis" containing hearsay if: "(A) the record was made at or near the time by—or from information transmitted by—someone with knowledge; (B) the record was kept in the course of a regularly conducted activity of a business, organization, occupation, or calling, whether or not for profit; (C) making the record was a regular practice of that activity; (D) all these conditions are shown by the testimony of the custodian or another qualified witness, or by a certification that complies with Rule 902(11) or (12) or with a statute permitting certification; and (E) the opponent does not show that the source of information or the method or circumstances of preparation indicate a lack of trustworthiness." Fed. R. Evid. 803(6). Rule 902(11), in turn, was adopted by amendment in 2000 to allow records of regularly conducted activity to be authenticated by certificate rather than by live testimony and provides that the proponent of a business record who meets certain notice requirements need not provide extrinsic evidence of authentication if the record meets the requirements of Rule 803(6)(A) through (C) "as shown by a certification of the custodian or another qualified person," Fed. R. Evid. 902(11); *see* Fed. R. Evid. 902 advisory committee's note (2000).

are not, and that any argument to the contrary misconceives the relationship between authentication and relevance, as well as the purpose of the business records exception to the hearsay rule.

First, to be admissible, evidence must be relevant, which means "its existence simply has some 'tendency to make the existence of any fact that is of consequence to the determination of the action more probable or less probable than it would be without the evidence.'" *United States v. Jones*, 566 F.3d 353, 364 (3d Cir. 2009) (quoting Fed. R. Evid. 401). Because evidence can have this tendency only if it is what the proponent claims it is, i.e., if it is authentic, *United States v. Rawlins*, 606 F.3d 73, 82 (3d Cir. 2010), "Rule 901(a) treats preliminary questions of authentication and identification as matters of conditional relevance according to the standards of Rule 104(b)," *United States v. Reilly*, 33 F.3d 1396, 1404 (3d Cir. 1994) (quoting Jack B. Weinstein & Margaret A. Berger, 5 Weinstein's Evidence ¶ 901(a)[01] at 901–15 (1993)).[6] Rule 104(b), in turn, provides that "[w]hen the relevance of evidence depends on whether a fact exists, proof must be introduced sufficient to support a finding that the fact does exist." Fed. R. Evid.

[6] Put differently, "[a]uthenticity is elemental to relevance." *Rawlins*, 606 F.3d at 82; *see* Fed. R. Evid. 901(a) advisory committee's note (1972) ("This requirement of showing authenticity or identity [under Rule 901(a)] falls in the category of relevancy dependent upon fulfillment of a condition of fact and is governed by the procedure set forth in Rule 104(b).").

104(b). We have determined that to meet the Rule 104(b) standard of sufficiency, the proponent of the evidence must show that "the jury could reasonably find th[ose] facts . . . by a preponderance of the evidence." *United States v. Bergrin*, 682 F.3d 261, 278 (3d Cir. 2012) (quoting *Huddleston v. United States*, 485 U.S. 681, 690 (1998)) (alterations in original); *see also United States v. Khorozian*, 333 F.3d 498, 506 (3d Cir. 2003) ("Authentication does not conclusively establish the genuineness of an item; it is a foundation that a jury may reject.").

Here, the relevance of the Facebook records hinges on the fact of authorship. To authenticate the messages, the Government was therefore required to introduce enough evidence such that the jury could reasonably find, by a preponderance of the evidence, that Browne and the victims authored the Facebook messages at issue. The records custodian here, however, attested only that the communications took place as alleged between the named Facebook accounts. Thus, accepting the Government's contention that it fulfilled its authentication obligation simply by submitting such an attestation would amount to holding that social media evidence need not be subjected to a "relevance" assessment prior to admission. Our sister Circuits have rejected this proposition in both the digital and non-digital contexts, as do we. *See United States v. Vayner*, 769 F.3d 125, 132 (2d Cir. 2014) (holding that a social media profile page was not properly authenticated where the government offered evidence only that the webpage existed and not that it belonged to the defendant); *United States v. Southard*, 700 F.2d 1, 23 (1st Cir. 1983) (observing that self-authentication "does not eliminate the requirement of relevancy" and requiring testimony linking the codefendant,

who had a common name, to the driver's license and work permit issued under that name).

The Government's theory of self-authentication also fails for a second reason: it is predicated on a misunderstanding of the business records exception itself. Rule 803(6) is designed to capture records that are likely accurate and reliable in content, as demonstrated by the trustworthiness of the underlying sources of information and the process by which and purposes for which that information is recorded.[7] *See E. C. Ernst, Inc. v. Koppers Co.*, 626 F.2d 324, 330–31 (3d Cir. 1980) (holding that pricing sheets satisfied Rule 803(6) because, among other things, "the sheets were checked for accuracy"); *see also United States v. Gurr*, 471 F.3d 144, 152 (D.C. Cir. 2006) ("Because the regularity of making the record is evidence of its accuracy, statements by 'outsiders' are not admissible for their truth under Fed. R. Evid. 803(6)."); Fed. R. Evid. 803 advisory committee's note (1972) ("The element of unusual reliability of business records is said variously to be supplied by systematic checking, by regularity and continuity which produce habits

[7] When we stated in *United States v. Console* that "Rule 803(6) does not require that the person transmitting the recorded information be under a business duty to provide accurate information," 13 F.3d 641, 657 (3d Cir. 1993), we were observing that accuracy need not be guaranteed, but in no way suggested that accuracy is irrelevant. On the contrary, we went on to state: "[I]t is sufficient if it is shown that . . . [the] standard practice was *to verify the information provided*, or that the information transmitted met the requirements of another hearsay exception." *Id.* at 657–58 (citations omitted) (alterations in original) (emphasis added).

of precision, by actual experience of business in relying upon them, or by a duty to make an accurate record as part of a continuing job or occupation.").

Here, Facebook does not purport to verify or rely on the substantive contents of the communications in the course of its business. At most, the records custodian employed by the social media platform can attest to the accuracy of only certain aspects of the communications exchanged over that platform, that is, confirmation that the depicted communications took place between certain Facebook accounts, on particular dates, or at particular times. This is no more sufficient to confirm the accuracy or reliability of the contents of the Facebook chats than a postal receipt would be to attest to the accuracy or reliability of the contents of the enclosed mailed letter. *See United States v. Jackson*, 208 F.3d 633, 637–38 (7th Cir. 2000) (holding that Internet Service Providers' ability to retrieve information that their customers posted online did not turn the posts that appeared on the website of a white supremacist group into the ISP's business records under Rule 803(6)); *cf. In re U.S. for Historical Cell Site Data*, 724 F.3d 600, 611 (5th Cir. 2013) (for Fourth Amendment purposes, defining business records as "records of transactions to which the record-keeper is a party," in contradistinction to "[c]ommunications content, such as the contents of letters, phone calls, and emails, which are not directed to a business, but simply sent via that business").

We have made a similar determination in the banking context. In *United States v. Furst*, 886 F.2d 558 (3d Cir. 1989), we held that the district court erred in admitting bank records as business records under Rule 803(6), even though the records verified the dates and amounts of certain deposits

and receipts, because "significant" other portions of these documents had not been independently verified, and the records custodians lacked "knowledge as to the accuracy of the information on which the [bank] documents was based or as to the knowledge of the persons who prepared the records." *Id.* at 572.

If the Government here had sought to authenticate only the timestamps on the Facebook chats, the fact that the chats took place between particular Facebook accounts, and similarly technical information verified by Facebook "in the course of a regularly conducted activity," the records might be more readily analogized to bank records or phone records conventionally authenticated and admitted under Rules 902(11) and 803(6). *See id.* at 573 (concluding that the district court erred in admitting bank statements in the bank's possession under Rule 803(6) "to the extent the statements contained any data other than confirmations of transactions" with the bank). We need not address the tenability of this narrow proposition here, however, as the Government's interest lies in establishing the admissibility of the chat logs in full. It suffices for us to conclude that, considered in their entirety, the Facebook records are not business records under Rule 803(6) and thus cannot be authenticated by way of Rule 902(11). In fact, the Government's position would mean that all electronic information whose storage or transmission could be verified by a third-party service provider would be exempt from the hearsay rules—a novel proposition indeed, and one we are unwilling to espouse.

B. Authentication by way of extrinsic evidence

Our conclusion that the Facebook chat logs were not properly authenticated under Rule 902(11) does not end our inquiry, for we may consider whether the Government has presented sufficient extrinsic evidence to authenticate the chat logs under Rule 901(a). *See Vatyan v. Mukasey*, 508 F.3d 1179, 1184 (9th Cir. 2007); *United States v. Dockins*, 986 F.2d 888, 895 (5th Cir. 1993). To answer this question, we look to what the rule means in the social media context and how it applies to the facts here.

Conventionally, authorship may be established for authentication purposes by way of a wide range of extrinsic evidence. *See* Fed. R. Evid. 901(b). In *United States v. McGlory*, 968 F.2d 309 (3d Cir. 1992), for example, we rejected a defendant's challenge to the authentication of notes that he had allegedly handwritten because, despite being unable to fully establish authorship through a handwriting expert, the prosecution had provided "sufficient evidence from which the jury could find that [the defendant] authored the notes." *Id.* at 329. The notes had been seized from the trash outside the defendant's known residences; some of the notes were torn from a notebook found inside his residences; some notes were found in the same garbage bag as other identifying information; and certain notes were written on note paper from hotels where the defendant stayed during the alleged conspiracy. *Id.* at 328–29.

Similarly, in *United States v. Reilly*, 33 F.3d 1396 (3d Cir. 1994), when considering whether the government's evidence "support[ed] the conclusion that the radiotelegrams are what the government claims they are, namely radiotelegrams to and from the *Khian Sea*, many of which

were sent or received by [the defendant]," we determined that the government had met its authentication burden by way of not only direct testimony from individuals who identified the radiotelegrams but also "multiple pieces of circumstantial evidence." *Id.* at 1405–06. This included testimony explaining how the witness who produced the radiotelegrams had come to possess them, the physical appearance of the radiotelegrams, and evidence that the radiotelegrams were sent to the defendant's office or telex number. *Id.* at 1406.

We hold today that it 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 consideration of the ways in which such data can be manipulated or corrupted, *see generally Lorraine v. Markel Am. Ins. Co.*, 241 F.R.D. 534 (D. Md. 2007), 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, *cf. Griffin v. State*, 19 A.3d 415, 424 (Md. 2011) (analyzing state analogue to Rule 901). But the authentication rules do not lose their logical and legal force as a result. *See Tienda v. State*, 358 S.W.3d 633, 638–39 (Tex. Crim. App. 2012) (describing the legal consensus as to the applicability of traditional evidentiary rules to electronic communications and identifying the many forms of circumstantial evidence that have been used to authenticate email printouts, internet chat room conversations, and cellular text messages); *see also Parker v. State*, 85 A.3d 682, 687 (Del. 2014) (analyzing state evidentiary rules and concluding that "[a]lthough we are mindful of the concern that social media evidence could be

falsified, the existing [rules] provide an appropriate framework for determining admissibility."); *Burgess v. State*, 742 S.E.2d 464, 467 (Ga. 2013) ("Documents from electronic sources such as the printouts from a website like MySpace are subject to the same [state] rules of authentication as other more traditional documentary evidence and may be authenticated through circumstantial evidence."). Depending on the circumstances of the case, a variety of factors could help support or diminish the proponent's claims as to the authenticity of a document allegedly derived from a social media website, and the Rules of Evidence provide the courts with the appropriate framework within which to conduct that analysis.

Those Courts of Appeals that have considered the issue have reached the same conclusion. In *United States v. Barnes*, 803 F.3d 209 (5th Cir. 2015), the Fifth Circuit held that the government laid a sufficient foundation to support the admission of the defendant's Facebook messages under Rule 901 where a witness testified that she had seen the defendant using Facebook and that she recognized his Facebook account as well as his style of communicating as reflected in the disputed messages. *Id.* at 217. In *United States v. Hassan*, 742 F.3d 104 (4th Cir. 2014), the Fourth Circuit held that the government properly linked the Facebook pages at issue to the defendants by using internet protocol addresses to trace the Facebook pages and accounts to the defendants' mailing and email addresses.[8] *Id.* at 133. And in *Vayner*, the Second

[8] The Fourth Circuit also ruled that those Facebook pages were properly authenticated under Rule 902(11). *Hassan*, 742 F.3d at 133–34. For the reasons already stated

Circuit held that the government failed to adequately authenticate what it alleged was a printout of the defendant's profile page from a Russian social networking site where it offered no evidence to show that the defendant had created the page. 769 F.3d at 131. In all of these cases, the courts considered a variety of extrinsic evidence to determine whether the government had met its authentication burden under Rule 901—each reiterating, in the course of that analysis, that conclusive proof of authenticity is not required and that the jury, not the court, is the ultimate arbiter of whether an item of evidence is what its proponent claims it to be. *Barnes*, 803 F.3d at 217; *Vayner*, 769 F.3d at 131; *Hassan*, 742 F.3d at 133.

Applying the same approach here, we conclude the Government provided more than adequate extrinsic evidence to support that the disputed Facebook records reflected online conversations that took place between Browne, Dalmida, and three of the four minors, such that "the jury could reasonably find" the authenticity of the records "by a preponderance of the evidence." *Bergrin*, 682 F.3d at 278.

First, although the four witnesses who participated in the Facebook chats at issue—Dalmida and three of the minors—did not directly identify the records at trial, each offered detailed testimony about the exchanges that she had over Facebook. This testimony was consistent with the content of the four chat logs that the Government introduced into evidence. Dalmida and two of the minors whose chat logs are at issue further testified that after conversing with the

---

above, we do not agree with this portion of the court's authentication holding.

Button Facebook account or the 998 number that they received through communications with Button, they met in person with Button—whom they were able to identify in open court as Browne. This constitutes powerful evidence not only establishing the accuracy of the chat logs but also linking them to Browne. *See United States v. Tank*, 200 F.3d 627, 630–31 (9th Cir. 2000) (holding government made a prima face showing of authenticity under Rule 901(a) in part because several co-conspirators testified that the defendant was the person who showed up to a meeting that they had arranged with the person who used that screen name).

Second, as reflected in the trial testimony of both Browne and Special Agent Blyden, Browne made significant concessions that served to link him to the Facebook conversations. Most notably, Browne testified that he owned the "Billy Button" Facebook account on which the search warrant had been executed and that he knew and had conversed on Facebook with Dalmida and two of the minors. *See, e g.*, *Tank*, 200 F.3d at 630–31 (holding government met authentication burden where, among other things, defendant admitted that screenname used in disputed text messages belonged to him). Browne also testified that he owned the phone that was seized from his residence—the same phone from which DHS recovered certain images that the victims identified on the stand as those they sent in response to commands from either the Button or Dalmida Facebook account or the 998 number. *Cf. United States v. Simpson*, 152 F.3d 1241, 1249–50 (10th Cir. 1998) (rejecting the defendant's claim that the trial court erred in admitting a printout of an alleged chat room discussion between the defendant and an undercover officer where, among other things, the pages seized from the defendant's home contained

identifying information that the undercover officer had given the individual in the chat room). And Browne admitted that he owned a second phone with the 344 number, which is significant because, although Browne attempted to distance himself from the incriminating phone with the 998 number with the unsupported contention that he loaned it to other individuals at various points in the relevant time period, one of the challenged Facebook conversations shows that "Button" also provided the 344 number to minor J.S. on two occasions while trying to elicit sexual acts and photos. In addition, in Browne's post-arrest statements, which were introduced at trial, he provided the passwords to the Button Facebook account and to the phone with the 998 number and admitted to exchanging nude photos with Dalmida, paying J.S. for nude photos, going to J.B.'s home, and knowing a third minor, T.P., whom he referenced by Facebook account name.

Third, contrary to Browne's contention that "there is no biographical information in the [Facebook] records that links [him] to the documents," Appellant's Br. at 17, the personal information that Browne confirmed on the stand was consistent with the personal details that "Button" interspersed throughout his Facebook conversations with Dalmida and three of the minors. For example, Browne testified that his address was 2031 Estate Lovenlund, that he was a plumber, and that he had a fiancée. The Facebook messages sent by "Button" are, in turn, replete with references to the fact that the sender was located or resided at Lovenlund. "Button" also stated to one minor, "I'm a plumber." App. 503. The chats reflect that somewhere on his Facebook profile, Button represented himself as being engaged. And in one of the

disputed Facebook chats, Button informed a minor that his name was "Tony . . . Browne."[9] App. 519.

Lastly, the Government not only provided ample evidence linking Browne to the Button Facebook account but also supported the accuracy of the chat logs by obtaining them directly from Facebook and introducing a certificate attesting to their maintenance by the company's automated systems. To the extent that certified records straight from the third-party service provider are less likely to be subject to manipulation or inadvertent distortion than, for instance, printouts of website screenshots, the method by which the Government procured the records in this case constitutes yet more circumstantial evidence that the records are what the Government claims.

---

[9] Browne argues that none of these biographical details constituted "information that only [he] could be expected to know," Appellant's Br. at 19, but we need not determine that, by itself, the information could suffice to authenticate the chat logs to conclude that they have some authentication value when considered in combination with all of the other available evidence. *See Simpson*, 152 F.3d at 1244 (computer printout of alleged chat room discussions properly authenticated not only by physical evidence recovered from defendant's home but also in light of the fact that the individual participating in the chat gave the undercover officer the defendant's first initial and last name and street address); *Bloom v. Com.*, 554 S.E.2d 84, 86–87 (Va. 2001) (defendant was sufficiently identified as individual who made statements over instant message where detailed biographical information provided online matched that of the defendant).

In short, this is not a case where the records proponent has put forth tenuous evidence attributing to an individual social media or online activity that very well could have been conducted or fabricated by a third party. *See, e.g.*, *Vayner*, 769 F.3d at 131; *see also Smith v. State*, 136 So.3d 424, 433 (Miss. 2014) (holding that name and photo on Facebook printout were not sufficient to link communication to alleged author); *Griffin*, 19 A.3d at 423 (holding that the trial court abused its discretion in admitting MySpace website evidence because the state both failed to explain how it had obtained the challenged records and failed to adequately link the records to the defendant's girlfriend). Far from it. This record reflects abundant evidence linking Browne and the testifying victims to the chats conducted through the Button Facebook account and reflected in the logs procured from Facebook. The Facebook records were thus duly authenticated.

Browne makes much of the fact that the Government failed to ask the testifying witnesses point-blank to identify the disputed Facebook chats. As we explained, however, in *McQueeney v. Wilmington Trust Co.*, 779 F.2d 916 (3d Cir. 1985), where we reversed the district court's determination that certain records could not be admitted into evidence unless they were introduced by a testifying witness, circumstantial evidence can suffice to authenticate a document. *Id.* at 928; *see also* Fed. R. Evid. 903 ("A subscribing witness's testimony is necessary to authenticate a writing only if required by the law of the jurisdiction that governs its validity."). Although a witness with personal knowledge may authenticate a document by testifying that the document is what the evidence proponent claims it to be, this is merely one possible means of authentication and not, as

Browne would have it, an exclusive requirement. *See* Fed. R. Evid. 901(b)(1); *Simpson*, 152 F.3d at 1249–50 (rejecting the defendant's contention that statements from a chat room discussion could not be attributed to him where the government could not identify that they "were in his handwriting, his writing style, or his voice," as "[t]he specific examples of authentication referred to by [the defendant] . . . are not intended as an exclusive enumeration of allowable methods of authentication").

In sum, Browne's authentication challenge collapses under the veritable mountain of evidence linking Browne to Billy Button and the incriminating chats.

C. Admissibility

Having concluded that the Facebook records were properly authenticated by way of extrinsic evidence, we turn to Browne's more general argument that the records were inadmissible. Evidence that is properly authenticated may nonetheless be inadmissible hearsay if it contains out-of-court statements, written or oral, that are offered for the truth of the matter asserted and do not fall under any exception enumerated under Federal Rule of Evidence 802. *McGlory*, 968 F.2d at 331.

Here, the Government offered more than sufficient evidence to authenticate four of the five Facebook records as chats that Browne himself participated in by way of the Button account, and these four records were properly admitted as admissions by a party opponent under Rule 801(d)(2)(A). *See id.* at 334 & n.17 (observing that handwritten notes were admissible as admissions by a party opponent if the prosecution established defendant's

authorship by a preponderance of the evidence); *see also United States v. Brinson*, 772 F.3d 1314, 1320 (10th Cir. 2014) (same conclusion regarding Facebook messages); *United States v. Siddiqui*, 235 F.3d 1318, 1323 (11th Cir. 2000) (same conclusion regarding authenticated email).[10] Not so for the fifth.

We agree with Browne that the single chat in which Browne did not participate and which took place between Dalmida and J.B. regarding Button's "almost rape[]" of J.B. was inadmissible hearsay. App. 483. Notwithstanding the other reasons the Government may have sought to admit it, the record functioned at least in part to prove the truth of the matter asserted, that is, that Browne sexually assaulted J.B. and subsequently threatened her with video evidence of the

[10] As for the statements in the chat logs that the victims made to Browne, under our precedent they were not hearsay because they were not offered into evidence to prove the truth of the matter asserted; rather, they were introduced to put Browne's statements "into perspective and make them intelligible to the jury and recognizable as admissions." *United States v. Hendricks*, 395 F.3d 173, 184 (3d Cir. 2005) (quoting *United States v. McDowell*, 918 F.2d 1004, 1007 (1st Cir. 1990)); *see also McDowell*, 918 F.2d at 1007–08 ("[The defendant's] part of the conversations was plainly not hearsay. Nor can a defendant, having made admissions, keep from the jury other segments of the discussion reasonably required to place those admissions into context . . . . Moreover, because [the informant's] statements were introduced only to establish that they were uttered and to give context to what [the defendant] was saying, they were not hearsay at all.").

assault. *See McGlory*, 968 F.2d at 332 ("This Court . . . has disfavored the admission of statements which are not technically admitted for the truth of the matter asserted, whenever the matter asserted, without regard to its truth value, implies that the defendant is guilty of the crime charged.").[11]

[11] As with authentication, we do not foreclose the possibility that the chat log might have warranted a different hearsay analysis had the Government sought the admission of only limited portions of it. In *United States v. Turner*, 718 F.3d 226 (3d Cir. 2013), for example, where we assessed the admissibility of certain bank records, we held that the district court did not clearly err in applying the residual hearsay exception, which permits a district court to admit an out-of-court statement not covered by Rules 803 or 804 where, among other things, "the statement has equivalent circumstantial guarantees of trustworthiness." *Id.* at 233 (quoting Fed. R. Evid. 807). But the Government here does not contend that this hearsay exception or any others enumerated in Rule 803 are applicable to this chat log. And with good reason. For instance, although the log reflects that the chat participants made a number of emotionally charged statements, it purports to describe an event that occurred the previous day and thus was not admissible under the present sense impression or excited utterance exception to the hearsay rule. Fed. R. Evid. 803(1)–(2); *see United States v. Green*, 556 F.3d 151, 156 (3d Cir. 2009); *United States v. Brown*, 254 F.3d 454, 458 (3d Cir. 2001). And nothing in the record or the Government's brief suggests the chat log was introduced to show Dalmida or J.B.'s "then-existing state of

Although we conclude that the District Court erred in admitting this chat log, we do not perceive grounds for reversal. Reversal is not warranted if it is "highly probable that the error did not contribute to the judgment." *United States v. Brown*, 765 F.3d 278, 295 (3d Cir. 2014) (quoting *United States v. Cunningham*, 694 F.3d 372, 391–92 (3d Cir. 2012)). This "high probability" standard for non-constitutional harmless error determinations "requires that the court possess a sure conviction that the error did not prejudice the defendant." *United States v. Franz*, 772 F.3d 134, 151 (3d Cir. 2014) (quoting *Cunningham*, 694 F.3d at 392).

We are confident there was no prejudice here. As detailed above, the Government set forth abundant evidence that not only served to tie Browne and the victims to the chat logs but also supported Browne's guilt on all of the counts for which he was convicted irrespective of those records. Indeed, the two individuals who made the hearsay statements reflected in the fifth chat log, Dalmida and J.B., testified at length to the very details included in that Facebook chat log. Because there was overwhelming, properly admitted evidence supporting Browne's conviction on every count, and the sole improperly admitted Facebook record was "at most, duplicative of [the witnesses'] admissible testimony," *United States v. Kapp*, 781 F.2d 1008, 1014 (3d Cir. 1986), the erroneous admission was harmless and Browne's convictions must be sustained. *See Barnes*, 803 F.3d at 218 (concluding that any potential error in admitting disputed Facebook messages was harmless, as "the content of the messages was

---

mind," Fed. R. Evid. 803(3). *See United States v. Donley*, 878 F.2d 735, 737 (3d Cir. 1989).

largely duplicative" of witness testimony and "given the overwhelming evidence of [the defendant's] guilt").

* * *

For the foregoing reasons, we will affirm the judgment of the District Court.