SUMMARY
October 3, 2019

**2019COA150**

**No. 18CA1613, *People v. N.T.B.* — Evidence — Admissibility — Authentication — Hearsay — Machine-generated Records — Hearsay Exceptions — Records of Regularly Conducted Activity**

A division of the court of appeals addresses the admissibility of evidence from a cloud storage account. First, the division holds that an investigating detective could provide sufficient background to authenticate records produced in response to a search warrant served on the cloud storage and internet service providers under CRE 901. Second, the division agrees with the trial court that because these records include statements that constitute hearsay, and because the prosecution had not listed a custodian to provide necessary foundation under CRE 803(6), they were inadmissible. The division distinguishes cases dealing with the

admissibility of electronic communications, such as emails and Facebook postings.

COLORADO COURT OF APPEALS **2019COA150**

---

Court of Appeals No. 18CA1613
El Paso County District Court No. 16CR4823
Honorable Robert L. Lowrey, Judge

---

The People of the State of Colorado,

Plaintiff-Appellant,

v.

N.T.B.,

Defendant-Appellee.

---

RULING APPROVED

Division III
Opinion by JUDGE WEBB
Dunn and Lipinsky, JJ., concur

Announced October 3, 2019

---

Daniel H. May, District Attorney, Oliver Robinson, Deputy District Attorney, Tanya A. Karimi, Deputy District Attorney, Colorado Springs, Colorado, for Plaintiff-Appellant

No Appearance for Defendant-Appellee

¶ 1 Evidence stored in an account on a remote cloud server raises novel questions of authentication and the business-records exception to the hearsay rule. The district attorney appeals the trial court's pretrial order dismissing all charges against N.T.B.[1] The court held that the prosecutor failed to present a witness to authenticate records of the cloud storage custodian and internet service provider, which were necessary to link N.T.B. to sexually exploitative material stored in the cloud. And even if the prosecution could have authenticated these records, the court held that they contained inadmissible hearsay. Because the prosecutor provided no basis for admitting them under the business-records exception, the trial court refused to admit them. We agree with the district attorney that the prosecutor proffered sufficient evidence of authenticity but reject his contention that the documents were not hearsay. Therefore, we approve the trial court's ruling.

## I. Background

¶ 2 Dropbox flagged a cloud-storage account that it suspected contained child pornography. The company provided the National

[1] N.T.B. has not entered an appearance in this court.

Center for Missing and Exploited Children with a video and an account identification number, an email address, account activity log, and internet protocol (IP) address tied to the upload.[2] The Center forwarded this information to local police.

¶ 3 The police served a search warrant on Dropbox, which produced everything stored in the account, and viewed the original video. They also viewed other videos that they believed contained sexually exploitative material, along with two still pictures of N.T.B., all of which were in the account.[3] The police traced the IP address to Comcast, the internet service provider, which identified a physical address for the internet account in response to a search warrant. The account was owned by N.T.B.'s then-girlfriend and his roommate.

---

[2] *People v. Garrison*, 2017 COA 107, ¶¶ 23-29, ¶ 24 n.3, explains that an IP number is a unique address assigned to a computer connected to the internet, and how an IP address can be traced to a residential address with information provided by an internet service provider. *See also United States v. Miller*, No. CV 16-47-DLB-CJS, 2017 WL 2705963, at *1 (E.D. Ky. June 23, 2017) (explaining how cloud storage providers identify suspected child pornography through "hashing" technology and report their findings to the Center).

[3] The videos, photographs, and activity log are not in the appellate record.

¶ 4 Next, the police executed a search warrant on their shared residence, where one detective interviewed N.T.B. He admitted to owning a Dropbox account associated with his work email address, which was the email address that Dropbox had provided, and watching pornography that others shared with him over Snapchat. But he did not confirm the account number.

¶ 5 The prosecution charged N.T.B. with three counts of sexual exploitation of a child under section 18-6-403(3)(b.5), C.R.S. 2019, based on his possession or control of pornographic videos in the account.

¶ 6 Before jury selection on the morning of trial, N.T.B. moved in limine to exclude all records obtained from Dropbox and Comcast, but not the videos. He argued that these documents were business records that contained hearsay, which would be admissible only if authenticated under either CRE 803(6) or by a certification that complied with CRE 902(11). The prosecutor had neither endorsed a records custodian to testify concerning the requirements of CRE 803(6) nor provided an affidavit and notice under CRE 902(11).

¶ 7 The prosecutor responded that the records could be authenticated under CRE 901(b)(1) and (4) based on testimony from

the investigating detective and distinctive information that connected N.T.B. to the Dropbox account obtained through the search warrants. He asserted that the records were not hearsay because "[t]here [was] no declarant" and that N.T.B. had admitted to owning a Dropbox account associated with his work email address.

¶ 8 After hearing arguments from defense counsel and the prosecutor, which included a proffer of the investigating detective's anticipated testimony, and taking a short recess to research the issue, the court ruled that the records would not be admissible at trial. It explained that "[t]here was no one to authenticate th[e] documents"; additionally, the court held that these documents were business records which contained hearsay.[4] And because the

[4] At one point, the court indicated, "[The prosecutor] has posed the notion that you can authenticate documents otherwise under [CRE] 901, specifically [Rule] 901(4). I suppose arguably that under [Rule] 901(b)(4) to 901(b)(1), testimony that the matter is what it is claimed to be . . . . Authentication can be accomplished by sufficient evidence to show that something is what it purports to be . . . ." A bit later, in the court's analysis of *People v. Marciano*, 2014 COA 92M-2, which was "the closest opinion [the court] found to the issue raised" in this case, the trial court adopted the *Marciano* court's business records rationale for exclusion.

prosecutor had not endorsed a custodian to testify nor provided an affidavit and notice, the trial court would not admit them.

¶ 9 The prosecutor conceded that without this evidence, the case could not be proven, and only twelve days remained before the speedy trial deadline would lapse. Then the court granted N.T.B.'s motion to dismiss and sealed the case.

## II. Jurisdiction and Standard of Review

¶ 10 Section 16-12-102(1), C.R.S. 2019, allows the prosecution to appeal a "final order" in a criminal case "upon any question of law." An order that dismisses one or more counts of a charging document before trial constitutes a final order. *Id.*; *see also People v. Gabriesheski*, 262 P.3d 653, 656-57 (Colo. 2011) (requiring appeals under section 16-12-102(1) to comply with the final judgment requirement of C.A.R. 1). And an evidentiary ruling may be appealed if the trial court made its ruling based on an allegedly erroneous interpretation of the law. *People v. Welsh*, 176 P.3d 781, 791 (Colo. App. 2007); *see also Gabriesheski*, 262 P.3d at 658 ("[I]t is enough here that [the prosecution's issues] posed questions of law and arose from decisions of a criminal court that had become final, within the contemplation of section 16-12-102(1) . . . .").

¶ 11 "Because we must always satisfy ourselves that we have jurisdiction to hear an appeal, we may raise jurisdictional defects sua sponte, regardless of whether the parties have raised the issue." *People v. S.X.G.*, 2012 CO 5, ¶ 9. We review questions of law de novo. *See People v. Ross*, 2019 COA 79, ¶¶ 2-10, 26.

¶ 12 The trial court held the Dropbox and Comcast records were business records that it could not admit without testimony or an affidavit from the custodians. *See* CRE 803(6), 902(11). The court made no findings of fact and did not weigh the evidence proffered by the prosecutor. Instead it relied entirely on its interpretation of the rules of evidence and relevant case law. So, while the district attorney is appealing an evidentiary ruling, that posture does not preclude appellate jurisdiction under section 16-12-102(1) when the question presented focuses on the proper application of the controlling legal standard. *Welsh*, 176 P.3d at 792; *see People v. McLeod*, 176 P.3d 75, 76 (Colo. 2008) (holding that a trial court's interpretation of the rape-shield statute presented an appealable question of law under section 16-12-102(1)); *see also People v. Medina*, 25 P.3d 1216, 1223 (Colo. 2001) (whether a statement constitutes hearsay is a legal conclusion).

¶ 13 In sum, we have jurisdiction to hear this appeal.

## III. Law

¶ 14 Principles of relevancy, authenticity, and hearsay govern the admissibility of computer-generated records. *People v. Huehn*, 53 P.3d 733, 736 (Colo. App. 2002).

### A. Relevancy

¶ 15 Only relevant evidence is admissible. CRE 402. Relevant evidence is evidence "having any 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." CRE 401.

### B. Authenticity

¶ 16 Authenticity is also a threshold requirement for admissibility. *People v. Baca*, 2015 COA 153, ¶ 26. The proponent may satisfy this requirement by presenting extrinsic evidence to show that the proffered evidence is what the proponent claims it to be under CRE 901. *Huehn*, 53 P.3d at 736. The burden to authenticate presents a low bar; "only a prima facie showing is required[.]" *People v. Glover*, 2015 COA 16, ¶ 13 (quoting *United States v. Hassan*, 742 F.3d 104, 133 (4th Cir. 2014)). Once the proponent

meets this burden, the actual authenticity of the evidence and the effect of any defects go to the weight of evidence and not its admissibility. CRE 104; *see People v. Lesslie*, 939 P.2d 443 (Colo. App. 1996).

¶ 17 CRE 901 does not definitively establish the nature or quantity of proof required to authenticate evidence. The trial court must make a fact-specific determination of whether the proof advanced is sufficient to support a finding that the item in question is what its proponent claims it to be. *See Colo. Citizens for Ethics in Gov't v. Comm. for Am. Dream*, 187 P.3d 1207, 1213 (Colo. App. 2008) ("Whether a proper foundation has been established is a matter within the sound discretion of the trial court . . . ."). CRE 901(b) contains a nonexhaustive list of methods to authenticate by extrinsic evidence. The list includes testimony by a witness with personal knowledge of the proffered evidence. CRE 901(b)(1).

¶ 18 As relevant here, where a law enforcement investigator possesses personal knowledge that proffered evidence was produced in response to a search warrant, courts have allowed the investigator to authenticate that evidence. *See, e.g.*, *United States v. Whitaker*, 127 F.3d 595, 601 (7th Cir. 1997) (holding that the

prosecution properly authenticated computer records seized during the execution of a search warrant through the testimony of the officer who retrieved them); *United States v. Sliker*, 751 F.2d 477, 488 (2d Cir. 1984) (allowing an investigating officer to authenticate bank documents obtained through a search warrant); *see also People v. Marciano*, 2014 COA 92M-2, ¶ 28 (cases from other jurisdictions with similar rules of evidence are instructive for interpreting Colorado Rules of Evidence).

¶ 19 Proponents tend to rely on CRE 901 to authenticate electronic communications such as emails, texts, and messages sent through social media platforms like Facebook. *See People v. Heisler*, 2017 COA 58, ¶¶ 15-23 (text messages); *Glover*, ¶¶ 21-34 (Facebook messages); *People v. Bernard*, 2013 COA 79, ¶¶ 7-13 (emails).

¶ 20 But unlike emails, texts, and social media messages, cloud-based files lack many of the readily identifiable characteristics that often make authentication under CRE 901 possible. Specifically, files uploaded to remote servers are not necessarily shared with other users, which forecloses the opportunity for a recipient to authenticate them. And cloud storage providers may not require detailed profiles of their users, which

eliminates another avenue to corroborate ownership of the account's contents.[5] *See generally Lorraine v. Markel Am. Ins. Co.*, 241 F.R.D. 534, 556-59 (D. Md. 2007) (discussing authentication issues for electronically stored information, and noting that "courts 'should . . . consider the accuracy and reliability of computerized evidence' in ruling on its admissibility.") (citation omitted).[6]

C. Hearsay

¶ 21 Authenticity does not guarantee admissibility. *See People v. Morise*, 859 P.2d 247, 250 (Colo. App. 1993) ("[T]he mere fact that a document is *authentic* does not mean that it is also *competent evidence* of the facts contained in that document."); *see also* Fed. R. Evid. 901(b) advisory committee's note to 1972 proposed rules

---

[5] Dropbox, for example, only requires a name, email address, and password to create a free account. *See* Dropbox, *Create an Account*, https://perma.cc/BX5T-S6KR.

[6] *See also* Scott A. McDonald, *Authenticating Digital Evidence from the Cloud*, Army Law. 40, 48 (2014) (concerning cloud storage, in "the absence of an acknowledgement of authorship and authenticity from a party with relevant knowledge . . . counsel should consider gathering additional circumstantial evidence of authenticity to satisfy the requirements of [Rule] 901"); Scott Moss & Ann England, *Evidentiary Foundation and ESI*, *in* Colo. Bar. Ass'n CLE, Information Security & Document Management 2/20 (July 25, 2018) (noting that presence on the internet does not suffice to establish authenticity; "the proponent must show that it came *from the person or entity* alleged to be the author or owner").

("[C]ompliance with requirements of authentication . . . by no means assures admission of an item into evidence, as other bars, hearsay for example, may remain[.]").

¶ 22 As relevant here, authentic evidence may be excluded on the basis that it is hearsay. *See* CRE 802. Hearsay "is a statement other than one made by the declarant while testifying at the trial or hearing, offered in evidence to prove the truth of the matter asserted." CRE 801(c). Still, not all computer-generated records constitute hearsay. Even if a party introduces a computer-generated record to prove the truth of its contents, that record may not constitute hearsay if the computer created the record automatically without human input or interpretation. *People v. Hamilton*, 2019 COA 101, ¶¶ 24-26.

¶ 23 In contrast to the low threshold for authentication, under which a court allows the jury to weigh questionably authentic evidence, a hearsay objection presents a binary choice — courts must exclude hearsay unless its proponent satisfies an exception. *Glover*, ¶ 37.

¶ 24 Our rules of evidence recognize exceptions to the general prohibition against admitting hearsay for certain inherently reliable

out-of-court statements. *See* CRE 803. One such exception allows courts to admit business records that meet criteria intended to ensure trustworthiness. *See Henderson v. Master Klean Janitorial, Inc.*, 70 P.3d 612, 617 (Colo. App. 2003) ("The business records exception is founded on a presumption of accuracy that exists because the information is reported by persons trained in the importance of precision and checked for its correctness, and because of the accuracy demanded by the nature of the business."). Hearsay subject to the business-records exception is

> [a] . . . report, record, or data compilation, in any form, of acts [or] events . . . made at or near the time by, or from information transmitted by, a person with knowledge, if kept in the course of regularly conducted business activity, and if it was the regular practice of that business activity to make the . . . report, record, or data compilation . . . .

CRE 803(6).

¶ 25 Examples of computer-generated records that have satisfied the business-records exception include invoicing data from billing software, activity records of an automated teller machine (ATM), credit card statements, and checking account statements. *State ex rel. Coffman v. Robert J. Hopp & Assocs., LLC*, 2018 COA 69M, ¶ 74

(invoicing data); *Marciano*, ¶¶ 24-31 (checking account statements); *Huehn*, 53 P.3d at 737-38 (ATM records); *People v. Berger-Levy*, 677 P.2d 351, 351-52 (Colo. App. 1983) (credit card statements).

¶ 26 Business records may contain statements made by third parties. Courts do not grant the same presumption of reliability to these statements because the third party does not have a duty to the business to report the information accurately. *Henderson*, 70 P.3d at 617. Still, third-party statements contained in business records are admissible under the business-records exception when the third party's information is provided as "part of a business relationship" between the business and third party, and evidence shows that the business "substantially relied" on the information. *People in Interest of R.D.H.*, 944 P.2d 660, 665 (Colo. App. 1997). But in *Glover*, ¶ 21, a division of this court held that Facebook messages were not admissible as a third-party statement in a business record because "even though an arguable business relationship exists between Facebook and its users, there was no evidence presented that Facebook substantially relies for any business purpose on information contained in its users' . . . communications."

## IV. Application

### A. Relevancy

¶ 27 Although the videos are not in the record, the probable cause affidavit describes the sexually explicit content of six of them and observes that the females depicted appear to be between five and thirteen years old. Thus, the relevancy of the Dropbox and Comcast records that identify the account containing the videos and connect N.T.B. to that account could not be disputed. *See* § 18-6-403(3)(b.5) (proscribing possession of or control over sexually exploitive material "for any purpose").

### B. Authenticity

¶ 28 The district attorney asserts that the trial court "found the Dropbox records would not be admissible because there was no one to authenticate" them, but that it erred "in failing to consider the prosecution's argument" about authentication. Whether the investigating officer's testimony provided a sufficient foundation from which the jury could reasonably find that the Dropbox and Comcast records were what the prosecution purported —

documents generated by these entities — presents a close question.[7]

¶ 29 The scant record shows that the trial court analyzed the pertinent rules and acknowledged that the prosecution might have authenticated the Dropbox and Comcast records under either CRE 901 or CRE 902. Thus, contrary to the district attorney's characterization, the trial court did consider the authentication argument.

¶ 30 Turning to the merits of the argument, we agree with the district attorney that the investigating officer's proffered testimony sufficed to support a finding that the records were what the prosecution asserted them to be, although we do so on different grounds than those argued by the district attorney on appeal. *See Thyssenkrupp Safway, Inc. v. Hyland Hills Parks & Recreation Dist.*, 271 P.3d 587, 589 (Colo. App. 2011) (An appellate court may affirm

[7] The district attorney's brief focuses exclusively on the Dropbox records, but because the Comcast record provides a step in the link between N.T.B. and the sexually exploitive material stored on Dropbox, we include it in our analysis, which applies equally to the Comcast records.

a trial court's ruling on "any grounds that are supported by the record.").

¶ 31 The district attorney's brief leans heavily on the holding in *Glover* that Facebook messages may not be authenticated and admitted under CRE 803(6) or CRE 902 because they were not business records of Facebook. But the argument that "the Dropbox records . . . are similar to the Facebook entries" only goes so far.

¶ 32 True, the pictures of N.T.B. and N.T.B.'s email address are arguably like Facebook messages insofar as they are all user-generated. But N.T.B. specifically objected to "the written documents" — i.e., the account identification number, the account activity log, and the IP address used to make the uploads — which were generated by Dropbox and Comcast and not the account user. On this point, we distinguish the business records at issue here from the Facebook messages in *Glover*.

¶ 33 But recall that CRE 901 is a flexible standard. The type and quantity of evidence necessary to authenticate a particular piece of evidence will always depend on context. For electronically stored information that lacks an acknowledgement or other indicia of authorship, persuasive authority suggests that the prosecution

should present evidence of accuracy and reliability to satisfy the requirements of CRE 901. *See Lorraine*, 241 F.R.D. at 558-59; Scott A. McDonald, *Authenticating Digital Evidence from the Cloud*, Army Law. 40, 48 (2014).

¶ 34 In this case, the prosecution proffered such evidence. The prosecutor made an offer of proof that the investigating detective would testify that he caused search warrants to be issued and served on Dropbox and Comcast; these entities provided him with the records in response to the warrants; and N.T.B. acknowledged to the detective that he owned a Dropbox account tied to his work email address. So, the investigating detective had sufficient personal knowledge indicating that the Dropbox and Comcast records were authentic. *See* CRE 901(b)(1).

¶ 35 Even so, the court properly recognized that the prosecution must overcome the hearsay objection.

C. Hearsay

¶ 36 The Dropbox account identification number, activity log, and associated IP address, as well as the Comcast records connecting the IP address to the physical address where N.T.B. resided, were offered for the truth of the information. Through these records,

Dropbox and Comcast asserted that these accounts existed, the Dropbox account was associated with N.T.B.'s email address, videos had been uploaded into that account at various times from a specific IP address, and the IP address was assigned to a Comcast account at a residential street address. Simply put, what these records *say* provided essential links between N.T.B. and the videos in the Dropbox account.

¶ 37 Recall, the district attorney asserts that these records do not constitute hearsay because "[t]here [was] no declarant." To the extent the district attorney is arguing that Dropbox and Comcast created the records automatically without human input or interpretation, this argument falls short for two reasons. First, as indicated, the Dropbox and Comcast records were not included in the record on appeal. When material portions of the record are omitted, we presume that they support the trial court's ruling. *See People v. Duran*, 2015 COA 141, ¶ 12. Second, and more importantly, the prosecutor's proffer before the trial court did not identify any basis for concluding that the records had been

generated automatically.[8] Thus, the records provided by Dropbox and Comcast may have included human-generated input and interpretation.

¶ 38 The district attorney argues that the trial court "misapplied the law" by holding that the Dropbox and Comcast records were business records "because they are content created by users, not the business" and because the substance of that content is not something upon which Dropbox "substantially relies." But Dropbox — not N.T.B. — generated the account identification number and account activity log in which it recorded the IP address. Like bank and credit card statements in *Marciano* and *Berger-Levy*, these records were a compilation of data created in the regular course of Dropbox's business.

¶ 39 On this basis, the records at issue here can be distinguished from the Facebook messages in *Glover*. There, the court relied on the party-admission exception to overcome the defendant's hearsay

[8] Consistent with *People v. Hamilton*, 2019 COA 101, this opinion does not preclude a party from offering evidence to show that computer records were generated automatically.

objection. By contrast, N.T.B. admitted only to owning a Dropbox account associated with his work email address.

¶ 40 So, the trial court correctly analogized the account number, activity log, and IP address to computer-generated account statements that other divisions have analyzed as business records in *Robert J. Hopp & Assocs.*, *Huehn*, *Berger-Levy*, and *Marciano*. And without testimony or an affidavit from the custodians showing that the records were made in the regular course of business, inputted accurately within a reasonable amount of time, and transmitted by a reliable person with knowledge, the trial court properly excluded these records.

¶ 41 The second part of the district attorney's argument — that Dropbox and Comcast do not "substantially rely" on their records — misapplies that legal test. This facet of the business record analysis applies only to information generated by a third-party. And of course, to maintain the integrity of numerous separate accounts, Dropbox and Comcast must rely on unique account numbers and IP addresses.

¶ 42 In the end, the trial court correctly held that the Dropbox and Comcast records contained inadmissible hearsay, essential to the

prosecutor's "possesses or controls" theory, which it could not admit without testimony from the records custodians or an affidavit.

## V. Conclusion

¶ 43 We approve the trial court's ruling.

JUDGE DUNN and JUDGE LIPINSKY concur.