IN THE

ARIZONA COURT OF APPEALS

DIVISION ONE

AMY SILVERMAN, et al.,
Plaintiffs/Appellants,

v.

ARIZONA HEALTH CARE COST CONTAINMENT SYSTEM,
Defendant/Appellee.

No. 1 CA-CV 21-0720
FILED 6-22-2023

Appeal from the Superior Court in Maricopa County
No. LC2021-000183-001
The Honorable Sara J. Agne, Judge

REVERSED AND REMANDED

COUNSEL

First Amendment Clinic Public Interest Law Firm, Phoenix
By Gregg P. Leslie, Jacob M. Karr, Zachary R. Cormier, Jack Prew-Estes*, Jake Nelson*, Maria McCabe*, Vanessa Stockwill*
Counsel for Plaintiffs/Appellants

Johnston Law Offices PLC, Phoenix
By Logan T. Johnston, III
Counsel for Defendant/Appellee

* Certified limited practice students. *See* Ariz. R. Sup. Ct. 39(c).

OPINION

Chief Judge Kent E. Cattani delivered the opinion of the Court, in which Acting Presiding Judge Cynthia J. Bailey and Vice Chief Judge David B. Gass joined.

CATTANI, Chief Judge:

¶1 This public records case presents a narrow issue of potentially broad import. Arizona law does not require a public entity to create any new record in response to a public records request. But does using encryption to redact non-disclosable information stored in an electronic database necessarily constitute creation of a new record? We hold that it does not.

¶2 This concept is particularly important in a case like this one, in which the public entity uses non-disclosable data as a critical part of its database structure (as the relational keys linking different tables). Thus, requiring the agency to use a one-way cryptographic hash function to redact the non-disclosable data—substituting a unique hashed value that masks protected *information* without destroying its *function* in the database—is necessary to ensure a requestor receives, to the extent possible, a copy of the real record. And because such encryption only hides a limited aspect of the record—without adding to, aggregating, analyzing, or changing any of the underlying information—it does not create anything new and does not result in the creation of a new record. Accordingly, and for reasons that follow, we reverse the superior court's dismissal of the journalists' public records lawsuit at issue here and remand for further proceedings consistent with this opinion.

FACTS AND PROCEDURAL BACKGROUND

¶3 The Arizona Health Care Cost Containment System ("AHCCCS") oversees the Arizona Long-Term Care System ("ALTCS"). Appellants Amy Silverman, Alex Devoid, and TNI Partners (d/b/a Arizona Daily Star) are journalists researching issues related to services for Arizonans with developmental disabilities, including those services provided by ALTCS. Appellants are seeking public records from AHCCCS to learn what factors affect eligibility decisions during the ALTCS application and screening process.

¶4 In February 2020, Appellants submitted a public records request for data in AHCCCS's databases for multiple categories of information provided in or related to ALTCS applications. Appellants acknowledged that healthcare-related information would have to be de-identified to comply with privacy rules under the Health Insurance Portability and Accountability Act ("HIPAA"). *See, e.g.,* 45 C.F.R. §§ 164.502(d), .514(a)–(c). Noting that the requested data might be contained in multiple tables, Appellants requested that, for de-identified data, AHCCCS "include a unique identifier, such as a hash key, to replace" information necessary to distinguish different individuals' records. Appellants' request expressly did not ask AHCCCS to "join tables together . . . or to conduct any type of analysis on the data," provided any existing relational keys remained intact.

¶5 The parties negotiated for over a year. Appellants narrowed their request, and AHCCCS agreed that substantial portions of the requested data could be provided. As relevant here, however, the agency asserted that HIPAA required redaction of each applicant's unique "AHCCCS ID," and because the databases used that unique identifier as a relational key connecting various tables across the databases, its removal would leave other elements of the requested data unlinked. Appellants asked that AHCCCS substitute a hashed value to hide the protected information while retaining the links, *see* 45 C.F.R. § 164.514(c), (b)(i)(R), but AHCCCS asserted that doing so would be creating a new record.

¶6 Given this impasse, Appellants filed a statutory special action to compel production of the requested public records with the substituted hashed values, *see* A.R.S. § 39-121.02(A), arguing that substituting a hashed value did not create a new record but rather operated as "an advanced, yet simply implemented, form of redacting identifying information." AHCCCS moved to dismiss for failure to state a claim, asserting that Appellants' request would require creation of new records—requiring AHCCCS "not only [to] search its databases but link its many tables and fields of data in ways they are not now linked." AHCCCS further asserted that fulfilling the request would be unduly burdensome and expressed concern that linking information across data fields would impermissibly risk re-identification of individual applicants.

¶7 Reasoning that "[r]eplacing redacted identifying numbers with new numbers, which the agency itself would have to select, is the creation of new records," the superior court granted the motion and dismissed the complaint. The court did not reach AHCCCS's undue burden and risk of re-identification arguments.

¶8 Appellants timely appealed, and we have jurisdiction under A.R.S. § 12-2101(A)(1).

DISCUSSION

¶9 We review de novo the superior court's dismissal of a complaint for failure to state a claim. *See* Ariz. R. Civ. P. 12(b)(6); *Coleman v. City of Mesa*, 230 Ariz. 352, 355–56, ¶¶ 7–8 (2012). Dismissal on this basis is appropriate only if the plaintiff "would not be entitled to relief under any interpretation of the facts susceptible of proof." *Coleman*, 230 Ariz. at 356, ¶ 8 (citation omitted); *Elm Ret. Ctr., LP v. Callaway*, 226 Ariz. 287, 289, ¶ 5 (App. 2010). We assume the truth of all well-pleaded factual allegations and all reasonable inferences therefrom, although "mere conclusory statements" do not suffice. *Coleman*, 230 Ariz. at 356, ¶ 9; *see also Jeter v. Mayo Clinic Ariz.*, 211 Ariz. 386, 389, ¶ 4 (App. 2005).

¶10 Under Arizona law, "[p]ublic records and other matters in the custody of any officer shall be open to inspection by any person at all times during office hours." A.R.S. § 39-121. This statutory mandate reflects Arizona's strong presumption in favor of open government and disclosure of public documents. *See Griffis v. Pinal County*, 215 Ariz. 1, 4, ¶ 8 (2007). Public policy favors subjecting agency action "to the light of public scrutiny" and ensuring that citizens are "informed about what their government is up to." *Scottsdale Unified Sch. Dist. No. 48 v. KPNX Broad. Co.*, 191 Ariz. 297, 302–03, ¶ 21 (1998) (citations omitted); *see also id.* at 300, ¶ 9 (noting that the public entity bears the burden to show a proper basis for withholding requested documents).

¶11 A requestor is generally entitled to review a copy of the "real record," even one maintained in an electronic format, *Lake v. City of Phoenix*, 222 Ariz. 547, 551, ¶ 13 (2009) (citation omitted), subject to redactions necessary to protect against risks to privacy, confidentiality, or the best interests of the state, *Carlson v. Pima County*, 141 Ariz. 487, 490–91 (1984); *Judicial Watch, Inc. v. City of Phoenix*, 228 Ariz. 393, 396, ¶ 12 (App. 2011). Thus, upon request, a public entity must search its electronic databases to identify and produce responsive records. *ACLU of Ariz. v. Ariz. Dep't of Child Safety*, 240 Ariz. 142, 144–45, 148–49, ¶¶ 1, 15, 17–18 (App. 2016). But the entity need not tally, compile, analyze, or otherwise provide information *about* the information contained in existing public records, which would in effect create a new record in response to the request. *Id.* at 145, 148–49, ¶¶ 1, 17–18. Nor is the entity required to compile the data in a form more useful to a requestor. *Id.* at 148–49, ¶¶ 17–18.

¶12 Here, Appellants proposed that AHCCCS could redact protected information that also served a functional purpose in the database structure by using a one-way cryptographic hash function, which would substitute a unique hashed value to mask the protected information without destroying its function. At AHCCCS's urging, the superior court held that "[r]eplacing redacted identifying numbers with new numbers, which the agency itself would have to select," would necessarily constitute creation of a new record. We disagree.

¶13 Using a one-way cryptographic hash function to substitute a unique hashed value for protected information does not add to or change any of the underlying information (much less aggregate or analyze the data); it just hides a limited aspect of it. Redaction-by-encryption does not create anything new, but rather represents a better-tailored redaction process that eliminates *only* information that is in fact protected. *Cf. ACLU Immigrants' Rights Project v. U.S. Immigr. & Customs Enf't*, 58 F.4th 643, 655 (2d Cir. 2023). Accordingly, we reverse the superior court's ruling granting AHCCCS's motion to dismiss.

¶14 We acknowledge that redaction-by-encryption is different than traditional redaction-by-deletion (or redaction-by-obscuring-text-behind-a-black-box), and it may only be feasible in the context of electronically stored records. But when public records are stored in that format, differences occasioned by newer forms of data storage may call for differences in how the data is disclosed. For example, embedded metadata is an inherent part of a public record maintained in an electronic format, even though such metadata was nonexistent and effectively meaningless for the same record stored on paper. *See Lake*, 222 Ariz. at 550–51, ¶¶ 13–15. Accordingly, applying redaction-by-encryption as a more tailored form of redaction (even if made possible only by electronic storage) serves to ensure that the requestor receives access to the "real record" to the greatest extent possible. *See id.* at 551, ¶ 13 (citation omitted); *Carlson*, 141 Ariz. at 490–91.

¶15 The most analogous authority construing the federal Freedom of Information Act ("FOIA") bears this out.[1] In *ACLU Immigrants' Rights Project v. U.S. Immigration & Customs Enforcement*, the government refused the ACLU's request to replace "A-Numbers"—a unique number assigned to each individual non-citizen immigrating to the United States, a

[1] Although Arizona's public records law is broader than the federal statute, Arizona courts look to FOIA for guidance. *Lunney v. State*, 244 Ariz. 170, 177, ¶ 21 n.8 (App. 2017).

number that is exempt from disclosure under FOIA—with an anonymized "Unique ID" that would permit the ACLU to track data related to individual (but unidentified) non-citizens across ICE's databases. 58 F.4th 643, 646 (2d Cir. 2023). The district court granted summary judgment for ICE on the basis that ACLU's requested substitutions required creation of new records. *Id.* at 646–47.

¶16 The Second Circuit reversed. *Id.* at 647. Although ICE maintained event-centric (rather than person-centric) databases, it also "chose[]—although it was not required—to have FOIA-exempt A-Numbers function as the sole 'key' or 'code' affording access to electronic data pertaining to individual [non-citizens] from its event-centric databases," and "ICE itself use[d] A-Numbers for that purpose." *Id.* at 647. "[D]istinguish[ing] between the *content* of an electronic record and the *function* it may have been assigned within a computer system," the court reasoned that although the A-Numbers themselves were properly redacted, the function they served was not. *Id.* at 656. ACLU's proposed substitution of Unique IDs—"numbers meaningless in themselves but able to perform the same access function as A-Numbers"—neither "alter[ed] the content of any exempt record" nor "document[ed] any new information" nor "otherwise create[d] any new records." *Id.* at 655–56. "Rather, Unique IDs serve[d] only . . . to preserve a function necessary to afford the public the same person-centric access to non-exempt records that ICE already has." *Id.* at 656.

¶17 Here, at least as alleged by Appellants, *see Coleman*, 230 Ariz. at 356, ¶ 9, AHCCCS uses protected information (presumably an individual's AHCCCS ID) as a relational key in AHCCCS's databases. *Compare ACLU Immigrants' Rights Project*, 58 F.4th at 646–47. Although the information itself is protected against disclosure, its functionality in the databases is not. *Compare id.* at 656. Using redaction-by-encryption to replace the protected information with an otherwise-meaningless hashed value does not add or change any information, it simply masks the protected information without forfeiting the access function AHCCCS has chosen to have it perform. *Compare id.* at 655–56.

¶18 We note that redaction-by-encryption does not entitle Appellants to anything more than the public record as it actually exists. Appellants' complaint alleged that AHCCCS uses protected information (which must be de-identified before production to comply with HIPAA requirements) as the relational keys providing existing links between tables. AHCCCS's contrary assertion that it cannot link the data appears to presuppose that the existing unique identifier used as a relational key would be blacked-out—that is, after redaction, the link would no longer exist. At this stage of proceedings and in light of Appellants' allegations, AHCCCS's position is essentially an assertion that it need not relink the data after breaking those links in the first instance. Appellants' request asks that AHCCCS not simply black-out the private information, but rather encrypt it so that the confidential aspect is hidden but the functional link remains intact.

¶19 Although Appellants' complaint could also be read to encompass a request for creation of new links, Appellants unequivocally conceded at oral argument before both the superior court and this court that they are seeking only preservation of *existing* links among the data, not creation of new links. *Cf. Clark Equip. Co. v. Ariz. Prop. & Cas. Ins. Guar. Fund*, 189 Ariz. 433, 439 (App. 1997) (a party's express, in-court concession "has the effect of a confessory pleading") (citation omitted).

¶20 Accordingly, to the extent the tables and fields in the existing databases (pre-redaction) are not in fact linked—and the record is not clear on that issue—AHCCCS is not required to create new links to serve Appellants' purposes. *See ACLU of Ariz.*, 240 Ariz. at 148, ¶ 17. But to the extent the links exist pre-redaction, all Appellants' complaint seeks, and what they are potentially entitled to, is preservation of those links that form part of the "real record." *See Lake*, 222 Ariz. at 551, ¶ 13 (citation omitted).

¶21 AHCCCS highlights several cases under FOIA and other states' public records law that it asserts support its position that redaction-by-encryption would constitute creation of a new record. But those cases arose in a meaningfully different procedural posture (involving consideration of a factual record) and involved analysis or manipulation of records far beyond the comparatively simple encryption proposed here.

¶22 For example, the court in *Center for Public Integrity v. F.C.C.* reasoned that requiring an entity to "replace [] redacted numbers with new numbers, which the [entity] itself would have to select" (rather than simply redacting a portion of each number) would require creation of a new record. 505 F. Supp. 2d 106, 114 (D.D.C. 2007). But the requestor's proposal there would have required the entity to divide numerical responses into ranges rather than disclose the numbers themselves. *Id.* That is, the proposal would have required the entity to *analyze* the numbers and provide the plaintiff information *about* the information contained in its records in the form of "modified data"—and that analytical step meant the proposal required the creation of a new record. *Id.*; *see also ACLU of Ariz.*, 240 Ariz. at 148–49, ¶¶ 17–18.

¶23 Likewise, the court in *Students Against Genocide v. Department of State* denied plaintiffs access to certain records because, although a public entity is required to provide "'any reasonably segregable,' non-exempt portion of an existing record" under FOIA, it need not create new documents. 257 F.3d 828, 837 (D.C. Cir. 2001) (quoting 5 U.S.C. § 552(b)). But unlike the instant case, that case involved a request for a new and different version of a public record. The plaintiffs there sought disclosure of spy satellite photos that were shown (but not distributed) by the United States Secretary of State during a closed-door session of the United Nations Security Council. *Id.* at 830. The plaintiffs argued that, even assuming disclosure of the photographs would compromise national security interests, the federal government should nevertheless be required to "produce new photographs at a different resolution" to mask the technical capabilities of the reconnaissance systems that took the photos. *Id.* at 837. Addressing the district court's grant of a motion for summary judgment in favor of the United States, the D.C. Circuit agreed with the government's position that the request was not for a limited redaction of private information within an existing record, but rather required modification of the record in its entirety to create a new image—to literally create a new record. *Id.* at 837–38.

¶24 The court in *Long v. Immigration & Customs Enforcement* reasoned that an entity need not create new links among existing data if the links did not originally exist. *See* No. 17-cv-1097 (APM), 2021 WL 3931879, at *4–5 (D.D.C. Sept. 2, 2021) (mem. op.). But as described above, *see supra* ¶¶ 18–20, when read in conjunction with Appellants' concessions, the instant complaint seeks only preservation of existing links, not the creation of new ones. Moreover, in *Long*, satisfying the request would have required complex supplemental data analysis "to manufacture complex and often imprecise connections between otherwise facially unrelated data" in a database. *Id.* Unlike the encryption requested here, this additional layer of data analysis, as well as the literal creation of new links, was what constituted the creation of a new record in *Long*. *Id.* at *5.

¶25 Finally, the court in *Sander v. State Bar of California* confirmed that an entity is not required to "recode its original data into new values" in order to de-identify personal identifying information. 237 Cal. Rptr. 3d 276, 289 (Cal. Ct. App. 2018). But that case addressed proposed methods for anonymizing data that were far more involved than the one-way encryption proposed here. *Id.* at 282–85. Each proposed method would have required the entity to "recode its original data into new values" by creating new groupings not contemplated in the existing database: e.g., grouping law schools into three classes, reorganizing race and ethnicity data into four instead of eight categories, and grouping "bands" of graduation years. *Id.* at 284, 289–90. Certain proposed anonymization methods would have required the entity to excise substantial portions of the database, then perform statistical computations on the remainder (after recoding the data) to generate new information. *Id.* at 284, 290. These proposed methods would have required the entity to literally "chang[e] the substantive content of an existing record or replac[e] existing data with new data." *Id.* at 291. It was the data manipulation and analysis to yield new records that provided information about the original data—and *not* the fact that the processes were intended to anonymize data while preserving existing links—that constituted creation of a new record. *See also ACLU of Ariz.*, 240 Ariz. at 148–49, ¶¶ 17–18.

¶26 The critical substantive distinction here is the absence of any request that AHCCCS analyze, compile, or otherwise manipulate its existing data to create a new record. *See id.* Masking private data through redaction-by-encryption in a way that hides the confidential information but retains any existing links between tables (to the extent they currently exist in AHCCCS's databases, *see supra* ¶¶ 18–20) is not creating anything new; it is just declining to obscure anything more than required.

¶27 Notably, none of these cases was decided on a motion to dismiss. *Center for Public Integrity*, *Students Against Genocide*, *Long*, and even *ACLU Immigrants' Rights Project* were decided on summary judgment, meaning the court could consider the facts surrounding the requestors' proposals. *Ctr. for Pub. Integrity*, 505 F. Supp. 2d at 108; *Students Against Genocide*, 257 F.3d at 830; *Long*, 2021 WL 3931879, at *1; *ACLU Immigrants' Rights Project*, 58 F.4th at 646–47. *Sander* was appealed after a five-day bench trial (largely focused on competing expert testimony about de-identification methods), which meant the trial court had a meaningful factual basis to assess the complications involved in de-identifying data. *See* 237 Cal. Rptr. 3d at 280–81. In contrast, the procedural posture here—AHCCCS's motion to dismiss—means that only basic principles relating to disclosure are in play. In this context, a court does not consider (and here, did not have) evidence bearing on potential factual issues such as whether Appellants' proposal would be unduly burdensome or would be insufficient to de-identify the data to the degree required by HIPAA (which AHCCCS asserts as alternative grounds to affirm). *See Coleman*, 230 Ariz. at 356, ¶¶ 8–9.

¶28 To be sure, the journalists' request may ultimately prove unduly burdensome given the scale of data involved, and redaction (by encryption and otherwise) may ultimately prove insufficient to adequately anonymize the data given the type of data requested. But those questions require evidentiary development and must be considered on their facts, not as questions of law. Accordingly, and given the standard required for dismissal prior to any evidentiary consideration, the superior court erred by concluding that Appellants' request necessarily involved creation of new records and by dismissing the complaint on that basis.

CONCLUSION

¶29 We reverse the dismissal and remand for further proceedings.

COURT OF APPEALS
STATE OF ARIZONA

AMY M. WOOD • Clerk of the Court
FILED: AA