

# Cybersecurity and Copyright Risks in Public Institutions

*an Issue Note*

Dian Ross, *RCI Digital Project Lead & Engineer*  
Jack Smye, *RCI Digital Lead Architect*

[info@rescast.com](mailto:info@rescast.com)

February 2026



*RCI Digital: a division of*

**RESEARCH** **CASTING** INTERNATIONAL

## Background

Public Galleries, Libraries, Archives, and Museums (GLAMs) are entrusted with the responsibility of preserving cultural treasures and artifacts, such as fossils, while also ensuring that these collections remain accessible and traceable. This responsibility has become increasingly challenging with the shift into the digital realm, which now includes ancillary data such as 3D scans. Exacerbating this challenge, rolling COVID-19 lockdowns (2020-2023) curtailed access to primary materials, resulting in an increased expectation of digital access to collections.

However, the digitization of collections and increased online access to institutions come with a significant risk: cybercrimes have surged across sectors [2], with public institutions, including museums, collectively recording tens of millions of attacks over a recent three-year period [3]. GLAMs are also considered to be at greater risk post-COVID, with the UK's Action Fraud team issuing a broad warning that ticket fraud was expected to rise as institutions reopened, especially due to their increased reliance on online systems [4].

## The Emerging Cybersecurity Risk

Following the rise in cyberattacks across sectors, GLAM institutions that have increased their reliance on online systems by adopting cloud-based services are facing increased risks. A notable example is the Blackbaud Cloud Storage Data Breach in May 2020 [5]. Blackbaud, which hosted approximately 25,000 clients at its peak, including many museums, announced in Spring 2020 that they had been the victim of a ransomware attack, compromising data from an estimated 13,000 clients. At the time, Blackbaud claimed that no personal or financial information had been exposed; however, this assurance was later proven false, leading to a \$49.5 million USD settlement with the U.S. Attorney General [6].

Since that attack, other incidents have further underscored the importance of secure backups for GLAM institutions. For example, on December 20, 2021, Gloucester City Council in the UK discovered a data breach attributed to a sleep malware virus linked to Russian hackers, which had been activated via a weblink sent to a councillor's email [7]. Two years later, their local museum was still unable to access its artifact database, and all servers had to be rebuilt at an estimated cost of £1 million [8].

More recently, ransomware attacks in October 2023 on both the British Library [9] and Berlin's Museum für Naturkunde (Natural History Museum) [10] compromised users' personal data and continue to disrupt both institutions' online catalogues. Similarly, the December 2023 cyberattack on Gallery Systems, a catalogue management software provider [11], affected more than 800 clients, including over 260 cultural institutions such as The Museum of Fine Arts, Boston, and Crystal Bridges Museum of American Art. The breach compromised access to Gallery Systems' proprietary software, TMS (The Museum System), which manages sensitive

information like donors, loans, and the locations of high-value artworks. The full extent of this breach has not yet been disclosed.

Finally, in October 2024, the Internet Archive and its Wayback Machine—often referred to as the "memory of the internet"—experienced three distributed denial of service (DDoS) attacks [12]. These attacks compromised over 31 million files and user passwords, resulting in multi-day service outages.

## **The Increasing Challenges of a Digital World**

Beyond cybersecurity, the rapid digitization of collections has introduced new challenges related to the ownership and authenticity of data. Prior to around 2013, most fossil specimens were reproduced using physical models or castings, which were protected by licensing restrictions. Unauthorized copies or alterations were effectively prevented due to the high cost, expertise required for casting, and the necessity of extended physical access to the specimen or its replica.

However, advancements in 3D imaging and printing technology have prompted the GLAM reproduction industry to adopt these new methods. While the digital shift offers valuable opportunities—such as the ability to 3D print objects that were previously impossible to replicate using traditional casting—it also presents a significant downside. The accessibility of technologies like 3D scanning on smartphones and hobbyist 3D printers has removed many of the legacy safeguards that physical molds once provided [13].

Moreover, in the fast-evolving world of 3D data, the emphasis on shareability over traceability on the contemporary internet has made it increasingly difficult to verify the validity and provenance of 3D scan files or attribute them to their rightful owners. Even with the efforts of digital rights organizations like Creative Commons, challenges persist. Additionally, this shift to digital representations has coincided with growing demands for open access to 3D scans and the repatriation of original objects. A significant development in this space occurred following the recent acquisition of Sketchfab by Fab, which led to a highly criticized business model that prioritizes commercial interests over those of original creators and current rights holders [14].

There are also now many examples of individuals creating their own scans of culturally significant pieces, often without the GLAMs' permission [10]. Perhaps the most prominent example of a collection object being scanned and shared without the consent of the GLAM is the Nefertiti bust held at Neues Museum in Berlin, Germany. In 2016, Berlin-based artists Nora Al-Badri and Jan Nikolai Nelles made headlines by publishing a complete, high-quality scan of the bust. Entitled "The Other Nefertiti," Al-Badri and Nelles alleged that they had made this scan in person in October 2015 using a Microsoft Kinect and that they were releasing it to the public to highlight concerns about foreign government ownership of cultural icons [15].

Although this scan was made freely available for those wanting to print their own copies, it inspired a debate regarding fair use and the monetization of 'publicly owned' objects. Further complicating the copyright situation is that, while Al-Badri and Nelles claimed to have created this 3D scan themselves, subsequent examination of the scan file indicated that the uploaded file may have been the Museum's own since the scan is far too detailed and of much higher quality than could be expected from a stealth capture by a Kinect [16].

Al-Badri and Nelles succeeded in raising awareness, and their artistic demonstration remains central to an ongoing debate within the Creative Commons community regarding open access and the repatriation of cultural treasures. A new art collective, Looty, has also placed itself at the intersection of these discussions by reclaiming 3D scans of African cultural artifacts to create non-fungible tokens (NFTs). Proceeds from these NFTs are then used to support contemporary artists of African heritage.

Amid these debates, some advocates have called for all 3D scans of cultural objects held by public institutions to be made freely available to the public. Cosmo Wenman, drawing on his experience with 3D scanning and printing, has become an "open access activist." He has submitted Freedom of Information (FOI) requests to GLAM institutions holding 3D files and has escalated to lawsuits when responses have not met his expectations [17]. One of his most significant cases, against the Musée Rodin [18] in Paris, was, according to his personal website, largely decided in his favor: the French court purportedly ruled that 3D scans are equivalent to administrative documents and should therefore be shared under FOI regulations for public institutions. However, as yet, this outcome has not been widely reported in traditional media.

## **The Evolving World of Copyright and Intellectual Property**

Crucially, as with many digital sectors, copyright law has struggled to keep pace with technological advancements, particularly in the area of 3D scans of fossil specimens. The question of whether a scan creates a new copyright term and rights holder, distinct from the original object, remains untested and unresolved. Some argue that because fossil specimens are natural objects, not human creations, they do not meet the fundamental originality requirement for copyright protection. If this argument holds, reproductions of such specimens may also be exempt from copyright claims.

However, a compelling case can be made for the copyrightability of fully reconstructed and infilled skeletal exhibits, which demonstrate originality through creative interpretation. This was recently tested during a Christie's auction in Hong Kong, where the copyright status of a reconstructed specimen was put to the test [19].

In November 2022, a Christie's auction of "Shen," a supposedly near-complete tyrannosaurus rex specimen, was canceled after paleontologist and president of Black Hills Institute of Geological Research in South Dakota, Pete Larson, asserted that the Shen dinosaur utilized

castings from another tyrannosaurus rex, “Stan,” to fill in significant gaps in the fossil specimen [20]. The Black Hills Institute holds the intellectual property rights for Stan and sells complete polyurethane replica casts for \$120k USD. While Christie’s claimed that approximately 80 of Shen’s bones were original, over 75% of the bones were ‘filled in’ with casts [21].

Originally expected to realize an auction price of \$31M USD, Shen was set to be the “star lot” before it was pulled from the auction, highlighting the growing interest in ‘genuine’ fossils and the subsequent fossil data (both as casts and as prints). With such high stakes, strong provenance tracking for this data becomes increasingly important—especially as the industry moves away from casting and more towards scanning and printing where the legacy safeguards may no longer apply.

Moving forward, it is uncertain whether traditional intellectual property laws will provide this protection to the owners of these scans, even with the argument that the creation of 3D scan data requires creative originality [22]. Copyright laws around the world are not uniform in interpreting what creative processes are protected; the future interpretation with regards to 3D scans is still ambiguous and as yet not legally tested.

## **Meeting the Emerging Challenges**

As services and collections increasingly migrate online, so, too, do opportunities for malicious actors to target system vulnerabilities. GLAMs have further unique challenges regarding balancing calls for digital preservation of collection objects coupled with increased requests for the repatriation of cultural treasures – including their digitized formats and particularly that of 3D scans. Legacy reliance on expensive reproduction equipment and untested legal grey areas regarding the copyright enforceability of copies, however, are not adequate to protect the integrity of GLAM collections as was demonstrated by the Nefertiti scan, and, with greatest relevance to the discussion of fossil specimen reproductions, the failed Shen dinosaur auction.

To meet these challenges and ensure the continued protection of its archive of 3D fossil specimen scans, RCI proposes a permissioned distributed ledger to establish the provenance and authenticity of such files. In this way, RCI seeks to establish an industry standard on the cataloguing of these replicas, establishing a ‘one true version’ of the 3D scans that can be confidently cited by the fossil community. Using a permissioned ledger environment will allow RCI oversight of its 3D fossil specimen scans while also allowing interested parties to attest to or query these files, with access via Creative Commons licenses and verifiable credentials.

It is RCI’s intention that this ledger will become a repository for all references to and uses of 3D scans of fossil specimens, and in doing this we will look to establish a gold standard of provenance tracking and the assurance of authentic data. To ensure tamper-resistance of the records, all such transactions involving the 3D scans will be cryptographically hashed before being written to the append-only ledger. Furthermore, the distributed hosting of this ledger will

address of a key concern of cybersecurity: ensuring duplicated, isolated backups to avoid the high cost associated with security breaches such as ransomware attacks that may lead to compromised privacy and loss of data.

In this first project stage, RCI is focusing on protecting Canadian cultural heritage and partnering with public institutions. Initially building upon its experience as one of the foremost providers museum-grade natural history specimens, particularly paleontological displays, RCI recognizes that this provenance tracking system can, and should, be applied to all cultural objects. When the Internet Archive was most recently hacked, the prevailing fear was that the internet has lost its memory [12]. Utilizing RCI's novel web3 provenance tracking system, it will be possible to automatically secure and authenticate the digital memory of GLAM collections while balancing institutional rights with public access, all while opening up a new world of digital opportunities.

# References

- [1] UNESCO/ PERSIST, "Guidelines for the Selection of Digital Heritage for Long Term Preservation," (2nd ed) May 2021. [Online]. Available: <https://unesdoc.unesco.org/ark:/48223/pf0000244280>. [Accessed October 2022].
- [2] AAG, "The Latest 2023 Cyber Crime Statistics (Updated October 2023)," October 2023. [Online]. Available: <https://aag-it.com/the-latest-cyber-crime-statistics/>. [Accessed October 2023].
- [3] I. Armstrong, "Museums and galleries cannot afford to ignore cybersecurity if they want to consolidate the success of their digital pivot," 3 August 2021. [Online]. Available: <https://www.museumnext.com/article/museums-and-galleries-cannot-afford-to-ignore-cybersecurity-if-they-want-to-consolidate-the-success-of-their-digital-pivot/>. [Accessed August 2023].
- [4] Action Fraud, "Beware of ticket fraud as restrictions ease," 14 June 2021. [Online]. Available: <https://www.actionfraud.police.uk/news/beware-of-ticket-fraud-as-restrictions-ease>. [Accessed September 2023].
- [5] J.Tidy, "Blackbaud hack: More UK universities confirm breach," 24 July 2020. [Online]. Available: <https://www.bbc.co.uk/news/technology-53528329>. [Accessed August 2023].
- [6] U.S. Securities and Exchange Commission, "SEC Charges Software Company Blackbaud Inc. for Misleading Disclosures About Ransomware Attack That Impacted Charitable Donors," 9 March 2023. [Online]. Available: <https://www.sec.gov/news/press-release/2023-48>. [Accessed September 2023].
- [7] Gloucester City Council, "Investigation concludes into cyber-attack on Gloucester City Council," 7 June 2023. [Online]. Available: <https://www.gloucester.gov.uk/about-the-council/news/2023-news/investigation-concludes-into-cyber-attack-on-gloucester-city-council/>. [Accessed August 2023].
- [8] C. Garcia, "Data breach concerns ahead of Gloucester cyber attack report," 18 April 2023. [Online]. Available: <https://www.bbc.co.uk/news/uk-england-gloucestershire-65301758>. [Accessed August 2023].
- [9] M. Banfield-Nwachi, "British Library suffering major technology outage after cyber-attack," *The Guardian*. [Online] <https://www.theguardian.com/books/2023/oct/31/british-library-suffering-major-technology-outage-after-cyber-attack> (Accessed 31 October 2023), 31 October 2023.
- [10] M. f. N. Berlin, "Information about the cyber attack on the Museum fur Naturkunde Berlin," 11 March 2024. [Online]. Available: <https://www.museumfuernaturkunde.berlin/en/information-about-cyber-attack-museum-fur-naturkunde-berlin>. [Accessed 10 May 2024].

- [11] M. Kan, "Software Used by Hundreds of Museums Taken Down by Ransomware Attack," *PC Solutions*. [Online] <https://www.pcmag.com/news/software-used-by-hundreds-of-museums-taken-down-by-ransomware-attack> (Accessed 10 May 2024), 4 January 2024.
- [12] L. Daniel, "Again - Third Cyber Attack in October 2024," *Forbes*. [Online] <https://www.forbes.com/sites/larsdaniel/2024/10/20/internet-archive-breached-again-third-cyber-attack-in-october-2024/> (Accessed Oct 21, 2024), 20 October 2024.
- [13] P. Oruç, "Rethinking Who 'Keeps' Heritage: 3D Technology, Repatriation and Copyright," *GRUR International*, vol. 71, no. 12, pp. 1138-1146, December 2022.
- [14] J. Batchelor, "Epic launches combined Fab marketplace amid confusion and backlash from artists and developers," *Games Industry.biz*. [Online] <https://www.gamesindustry.biz/epic-launches-combined-fab-marketplace-amid-confusion-and-backlash-from-artists-and-developers> (Accessed 23 October 2024), 22 October 2024.
- [15] J. N. Nelles, "The Other Nefertiti," 2015. [Online]. Available: <https://aloversky.com/puzzlepieces/the-other-nefertiti>. [Accessed 23 August 2023].
- [16] C. Wenman, "The Nefertiti 3D Scan Heist is a Hoax," 13 November 2019. [Online]. Available: <https://cosmowenman.com/2016/03/08/the-nefertiti-3d-scan-heist-is-a-hoax/>. [Accessed 23 August 2023].
- [17] C. Wenman, "Cosmo Wenman," [Online]. Available: <https://cosmowenman.com/>. [Accessed 23 October 2024].
- [18] C. Wenman, "Secret 3D Scans in the French Supreme Court," 29 September 2024. [Online]. Available: <https://cosmowenman.substack.com/p/secret-3d-scans-in-the-french-supreme>.
- [19] J. J. a. Z. Small, "Christie's Pulls T. Rex From Auction, Citing Need for 'Further Study'," 20 November 2022. [Online]. Available: <https://www.nytimes.com/2022/11/20/arts/christies-t-rex-shen-stan.html>. [Accessed July 2023].
- [20] E. Feldman, "Christie's Calls Off T. Rex Auction Expected to Fetch \$25 Million," 22 November 2022. [Online]. Available: <https://www.smithsonianmag.com/smart-news/christies-calls-off-t-rex-auction-expected-to-bring-in-25-million-180981167/>. [Accessed 23 August 2023].
- [21] A. Binley, "T. rex auction cancelled after skeleton doubts raised," BBC, 21 November 2022. [Online]. Available: <https://www.bbc.com/news/world-asia-63700297>. [Accessed 23 August 2023].
- [22] C. Dunn, "Scanning Cultural Heritage: The Implications for Intellectual Property and Cultural Institutions," *Art, Antiquity and Law*, vol. 25, no. 1, pp. 25-54, 2020.
- [23] M. Weinberg, "3D Scanning: A World Without Copyright," May 2016. [Online]. Available: <https://michaelweinberg.org/docs/white-paper-3d-scanning-world-without-copyright.pdf>. [Accessed 23 August 2023].

- [24] P. Clammer, "Erasing Isis: how 3D technology now lets us copy and rebuild entire cities," 16 May 2016. [Online]. Available: <https://www.theguardian.com/cities/2016/may/27/isis-palmyra-3d-technology-copy-rebuild-city-venice-biennale>. [Accessed September 2023].
- [25] H. J. a. T. Solomon, "Greece Rejects Possibility of Parthenon Marbles 'Loan' in New Statement," 6 January 2023. [Online]. Available: <https://www.artnews.com/art-news/news/greece-rejects-parthenon-marbles-loan-plan-statement-1234652854/>. [Accessed September 2023].
- [26] S. McIntosh, "British Museum was victim of inside job, George Osborne says," 18 October 2023. [Online]. Available: <https://www.bbc.co.uk/news/entertainment-arts-67144607>. [Accessed October 2023].
- [27] M. Solly, "This Replica of a Tlingit Killer Whale Hat Is Spurring Dialogue About Digitization," Smithsonian Magazine, 11 September 2017. [Online]. Available: <https://www.smithsonianmag.com/smithsonian-institution/replica-tlingit-killer-whale-hat-spurring-dialogue-about-digitization-180964483/>. [Accessed 23 August 2023].