Balancing Accessibility and Security: Safeguarding Citizen-Sourced Biodiversity Data in the Age of AI and Open-Sourced Software

Nathan Fox [1,2,*], Enrico Di Minin [3], Neil Carter [2], Sabina Tomkins [4], Derek Van Berkel [2]

1. Michigan Institute for Data & AI in Society, University of Michigan
2. School for Environment and Sustainability, University of Michigan
3. Department of Geosciences and Geography, University of Helsinki
4. School of Information, University of Michigan

*Corresponding author email: foxnat@umich.edu

Summary
Artificial Intelligence (AI) and open-source software are revolutionizing biodiversity monitoring by democratizing access to citizen-science datasets. While these advancements facilitate conservation efforts and scientific research, they pose significant risks for data misuse. Researchers who reduce barriers to accessing such biodiversity datasets are responsible for safeguarding sensitive data.

Main Text
In recent years, the rise of mobile applications like iNaturalist (*inaturalist.org*) and eBird (*ebird.org*), coupled with the ubiquity of social media platforms such as Flickr (*flickr.com*) and Instagram (*instagram.com*), has led to an explosion of citizen-sourced biodiversity data (Ghermandi et al., 2023; Toivonen et al., 2019). These platforms allow the public to voluntarily and involuntarily contribute to scientific research by sharing observations of species, often accompanied by geotagged photographs and detailed textual descriptions. This democratization of data collection is revolutionizing biodiversity monitoring, enabling scientists and conservationists to gather vast amounts of information about species distributions, behaviors, and trends across the globe (Barve, 2014; Fox et al., 2020).

Open-source software has become a cornerstone of modern biodiversity research, providing researchers worldwide with the tools to extract and analyze data from multiple sources. These tools enable the creation of large, comprehensive datasets, often at reduced cost (Fox et al., 2020; Ghermandi et al., 2023). Meanwhile, AI algorithms have unlocked new possibilities for species identification, allowing for the rapid processing of vast amounts of citizen-sourced data from platforms like iNaturalist, eBird, and social media sites (August et al., 2020; Fox et al., 2024). AI algorithms can go beyond species identification, enabling the tracking of species movements, monitoring animal behavior, and detecting trends in near-real time that may be impossible to discern manually (Fox & Van Berkel, 2024; Tuia et al., 2022).

While the accessibility of this data has fueled innovation and collaboration in the conservation community, it has also introduced significant risks. The same data that helps researchers monitor biodiversity can be exploited by malicious actors such as poachers and illegal wildlife traders (Figure 1). High-resolution images and geotagged data can inadvertently reveal precise

and nearly real-time locations of rare and vulnerable species (Bergman et al., 2022). With reduced time lags between data upload and analysis, these tools could unintentionally aid malicious actors in mobilizing faster. Additionally, the collection of biodiversity data often includes incidental information about individuals, such as people appearing in photos taken in natural settings, raising significant privacy concerns as these individuals could be exposed to legal or social risks (Di Minin et al., 2021).

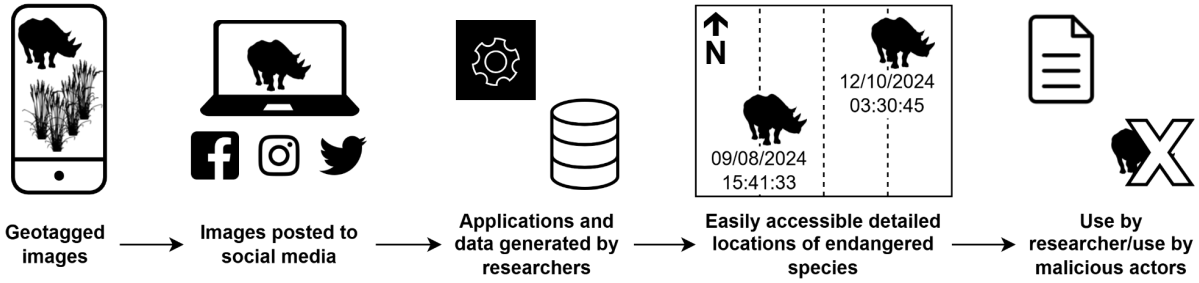

Figure 1. Pipeline for generating accessible datasets of endangered species locations from georeferenced images uploaded to social media. The improved data access for detailed locations is shared between researchers and potential malicious actors alike.

Who is Responsible For Safeguarding Data?

As open-source software and AI algorithms become more prevalent in biodiversity monitoring, the dual challenge of balancing accessibility and safeguarding sensitive data becomes particularly evident. One could argue that the responsibility of safeguarding these data lies with the citizen-science platforms used for biodiversity monitoring themselves, as is evident with several social media community guidelines that expressly prohibit these activities. For example, the Instagram community guideline states, '*No one may coordinate poaching or selling of endangered species or their parts*' (help.instagram.com). However, community guidelines alone will not prevent data misuse from malicious actors. While some biodiversity-focused citizen sites have protocols for data safeguards, such as eBird providing mechanisms for hiding data on sensitive species from the public (Lennox et al., 2020), social media platforms often lack robust safeguards against the misuse of the sensitive data they host. The absence of built-in protections does not absolve researchers of their responsibility to ensure that the data they create, use, and share does not facilitate harm. Making it easier to access and use these data without considering potential consequences could inadvertently contribute to the threats to biodiversity and people that we seek to combat (Ghermandi et al., 2023). Researchers must recognize their ethical obligations and take proactive steps to mitigate risks, even if the platforms themselves do not enforce these protections.

Safeguarding Strategies

When developing open-source tools for data extraction for biodiversity monitoring, researchers must prioritize the protection of sensitive data. These tools should be designed to selectively extract only the necessary data needed for biodiversity monitoring, focusing on non-sensitive information rather than indiscriminately scraping all available data (Di Minin et al., 2021). While accessing data, researchers should also pay close attention to data licenses, ensuring its utilization is in accordance with the terms of use (August et al., 2020). Implementing such

standards when obtaining data can significantly reduce the risk of sensitive information being processed or inadvertently shared further down the line.

To mitigate these risks introduced by AI annotations, researchers should first enhance data vetting and validation processes (Soriano-Redondo et al., 2024). Before potentially sensitive data is shared or published, it should undergo a thorough review to ensure that it does not contain any misinformation or information that could be exploited for harmful purposes. AI can be employed to flag potentially sensitive information, allowing it to be reviewed by human experts before being finalized. Furthermore, these systems should attempt to reduce misclassifications by flagging uncertain predictions that can again be reviewed (August et al., 2020).

In cases where access privately by researchers to sensitive data is necessary, the use of secure, encrypted databases to store this information, ensuring that only authorized personnel can access it, should be sufficient to protect it (Lennox et al., 2020). However, when research data needs to be made open-access or shared, particularly where requested by funders or journals, anonymization and pseudonymization protocols should be developed to remove or obscure personal information from images and datasets, thereby protecting individuals' privacy (Di Minin et al., 2021; Soriano-Redondo et al., 2024). AI can assist in this process by automatically detecting and blurring faces or other identifiable features in images and text before they are made publicly accessible. Further, data generalization techniques (i.e., decreasing spatial resolution) can obscure precise locations while providing useful information for conservation efforts (Lennox et al., 2020).

Researchers should consider how and when they release their generated data. For instance, if working with real-time sightings, researchers could impose time delays on access, particularly concerning the locations of endangered species (Lennox et al., 2020). By introducing time delays in the release of such data, the risk of poaching can be significantly reduced. Moreover, researchers should consider implementing tiered access systems, where different data sensitivity levels are associated with corresponding access permissions. This way, less sensitive data can be available for broader use, while more sensitive information remains protected. Moreover, spatial data involving highly sensitive information on endangered or species targeted by poachers should be withheld from open-access sources to prevent potential misuse. In the case of research including figures showing the locations of these species, methods, such as Privacy-Preserving Data Mining, can be used to effectively protect the location of the species while still retaining the knowledge contained in the original data.

Moving Forward

This work does not capture the full range of safeguarding measures a researcher can implement, but is designed to highlight the responsibility the researcher carries when creating and sharing such data. As we move forward, researchers should advocate for the development of ethical frameworks and guidelines for the use of biodiversity data from citizen-sourced datasets (Chowdhury et al., 2024). These frameworks should emphasize the importance of data protection and responsible use, and they should be developed in collaboration with a wide

range of stakeholders, including conservationists, technologists, legal experts, and representatives from local communities, as well as with funders that increasingly require that data be publicly shared upon manuscript publication. It is therefore important that researchers engage in dialogue with these data providers to ensure the implementation of controlled access and robust data-sharing policies, which are essential for balancing transparency with security (Ghermandi et al., 2023; Soriano-Redondo et al., 2024).

Creating AI-validated biodiversity sightings and open-source software for accessing and processing these datasets offers significant benefits, but it also comes with inherent risks. By implementing strategic safeguards and fostering a collaborative, ethical approach to data management, we can harness these technologies for the greater good while minimizing the potential for harm. Balancing accessibility with security will be crucial in ensuring that the advancements in biodiversity monitoring contribute positively to conservation efforts without inadvertently endangering the very species we aim to protect.

References

August, T. A., Pescott, O. L., Joly, A., & Bonnet, P. (2020). AI Naturalists Might Hold the Key to Unlocking Biodiversity Data in Social Media Imagery. *Patterns*, *1*(7). https://doi.org/10.1016/j.patter.2020.100116

Barve, V. (2014). Discovering and developing primary biodiversity data from social networking sites: A novel approach. *Ecological Informatics*, *24*, 194–199. https://doi.org/10.1016/j.ecoinf.2014.08.008

Bergman, J. N., Buxton, R. T., Lin, H.-Y., Lenda, M., Attinello, K., Hajdasz, A. C., Rivest, S. A., Tran Nguyen, T., Cooke, S. J., & Bennett, J. R. (2022). Evaluating the benefits and risks of social media for wildlife conservation. *FACETS*, *7*, 360–397. https://doi.org/10.1139/facets-2021-0112

Chowdhury, S., Ahmed, S., Alam, S., Callaghan, C. T., Das, P., Di Marco, M., Di Minin, E., Jarić, I., Labi, M. M., Rokonuzzaman, Md., Roll, U., Sbragaglia, V., Siddika, A., & Bonn, A. (2024). A protocol for harvesting biodiversity data from Facebook. *Conservation Biology*, *38*(4), e14257. https://doi.org/10.1111/cobi.14257

Di Minin, E., Fink, C., Hausmann, A., Kremer, J., & Kulkarni, R. (2021). How to address data privacy concerns when using social media data in conservation science. *Conservation*

Biology, *35*(2), 437–446. https://doi.org/10.1111/cobi.13708

Fox, N., August, T., Mancini, F., Parks, K. E., Eigenbrod, F., Bullock, J. M., Sutter, L., & Graham, L. J. (2020). “photosearcher” package in R: An accessible and reproducible method for harvesting large datasets from Flickr. *SoftwareX*, *12*, 100624. https://doi.org/10.1016/j.softx.2020.100624

Fox, N., Di Minin, E., Carter, N., Tomkins, S., & Van Berkel, D. (2024). Artificial Intelligence and Crowdsourced Social Media Data for Biodiversity Monitoring and Conservation. In A. Olanrewaju & S. Bruno (Eds.), *Advancements in Architectural, Engineering, and Construction Research and Practice* (pp. 43–50). Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-59329-1_4

Fox, N., & Van Berkel, D. (2024). Identifying invasive species sightings from GeoAI-validated social media posts. *I-GUIDE Forum 2024: Convergence Science and Geospatial AI for Environmental Sustainability*. I-GUIDE Forum. https://doi.org/10.5703/1288284317801

Ghermandi, A., Langemeyer, J., Van Berkel, D., Calcagni, F., Depietri, Y., Egarter Vigl, L., Fox, N., Havinga, I., Jäger, H., Kaiser, N., Karasov, O., McPhearson, T., Podschun, S., Ruiz-Frau, A., Sinclair, M., Venohr, M., & Wood, S. A. (2023). Social media data for environmental sustainability: A critical review of opportunities, threats, and ethical use. *One Earth*, *6*(3), 236–250. https://doi.org/10.1016/j.oneear.2023.02.008

Lennox, R. J., Harcourt, R., Bennett, J. R., Davies, A., Ford, A. T., Frey, R. M., Hayward, M. W., Hussey, N. E., Iverson, S. J., Kays, R., Kessel, S. T., Mcmahon, C., Muelbert, M., Murray, T. S., Nguyen, V. M., Pye, J. D., Roche, D. G., Whoriskey, F. G., Young, N., & Cooke, S. J. (2020). A Novel Framework to Protect Animal Data in a World of Ecosurveillance. *BioScience*, *70*(6), 468–476. https://doi.org/10.1093/biosci/biaa035

Soriano-Redondo, A., Correia, R. A., Barve, V., Brooks, T. M., Butchart, S. H. M., Jarić, I., Kulkarni, R., Ladle, R. J., Vaz, A. S., & Minin, E. D. (2024). Harnessing online digital data in biodiversity monitoring. *PLOS Biology*, *22*(2), e3002497.

https://doi.org/10.1371/journal.pbio.3002497

Toivonen, T., Heikinheimo, V., Fink, C., Hausmann, A., Hiippala, T., Järv, O., Tenkanen, H., & Di Minin, E. (2019). Social media data for conservation science: A methodological overview. *Biological Conservation*, *233*, 298–315. https://doi.org/10.1016/j.biocon.2019.01.023

Tuia, D., Kellenberger, B., Beery, S., Costelloe, B. R., Zuffi, S., Risse, B., Mathis, A., Mathis, M. W., van Langevelde, F., Burghardt, T., Kays, R., Klinck, H., Wikelski, M., Couzin, I. D., van Horn, G., Crofoot, M. C., Stewart, C. V., & Berger-Wolf, T. (2022). Perspectives in machine learning for wildlife conservation. *Nature Communications*, *13*(1), 792. https://doi.org/10.1038/s41467-022-27980-y