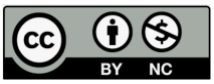
This is an Accepted Manuscript of an article published by Taylor & Francis in *Serials Librarian* on March 8, 2021, available online:
http://www.tandfonline.com/doi/full/10.1080/0361526X.2021.1875959
https://doi.org/10.1080/0361526X.2021.1875959

Privacy and Research Information Management Systems

Megan Macken and Clarke Iakovakis

Oklahoma State University Library



This paper is a case study of privacy considerations in the adoption of a Research Information Management (RIM) Systems. RIM Systems collect, store, and link together metadata for research, service, grants, and teaching activity. Sometimes called Current Research Information Systems (CRIS) or Faculty Activity Reporting (FAR), these systems enable institutions to collect data from different internal systems and combine it with external information, providing a more holistic perspective on university activity. They provide a single, authoritative source of this data and allow for multiple stakeholders (i.e. faculty, administration, IT, HR, library, communications) to query, analyze, download, visualize, and share it. Oklahoma State University (OSU) recently adopted a RIM System, which is being implemented and supported by the OSU Libraries. A defining factor in the decision making process for product selection was how each system addressed issues around privacy. This case study will review some of the central data privacy considerations at play in the adoption of RIM Systems at both the institutional and individual level. This will include data sharing, ownership, retention, right to reuse data, data deletion obligations upon contract termination, user access to privacy policies, and user data controls. Questions to ask before adoption, key institutional players in discussions of privacy, and issues that may arise after adoption of a Research Information Management System will also be addressed.

Keywords: research information management systems; privacy; library systems; privacy policies; data sharing; data ownership; data retention; researcher data; researcher profiles

Introduction

A Research Information Management System (RIM System) is a software platform for the collection, storage, and linking together of metadata related to faculty service, grants, teaching, and scholarly activities. European universities began developing RIM Systems in the 1990s, predominately to help them meet government reporting requirements.[1] A number of open source and proprietary RIM Systems have since been developed and many universities across the globe have either adopted one of these tools, or created their own RIM Systems.[2] Concurrently, these tools have increased in functionality; for instance, offering automated data feeds from institutional systems, automated publications harvesting, ORCiD read/write integration, sophisticated reporting tools, connection to institutional repositories, public profile options, and more. Commercial RIM Systems include Symplectic Elements (Digital Science), Pure (Elsevier), and Converis (Clarivate Analytics); open source systems include VIVO and DSpace-CRIS.[3]

---

[1]Bryant, Rebecca, Anna Clements, Pablo de Castro, Joanne Cantrell, Annette Dortmund, Jan Fransen, Peggy Gallagher, and Michele Mennielli, *Practices and Patterns in Research Information Management: Findings from a Global Survey*," (Dublin, OH: OCLC Research, 2018), doi: 10.25333/BGFG-D241

[2] David Scherer, Kate Byrne, Mark Hahnel, and Daniel Valen, "Collaborative Approaches to Integrate Repositories within the Research Information Ecosystem: Creating Bridges for Common Goals," *The Serials Librarian* 78, no. 1–4 (June 1, 2020): 181–90, doi: 10.1080/0361526X.2020.1728169.

[3] Wikipedia contributors, "Comparison of research networking tools and research profiling systems," *Wikipedia, The Free Encyclopedia,* accessed July 1, 2020, https://en.wikipedia.org/wiki/Comparison_of_research_networking_tools_and_research_profiling_systems.

As developers have added functionality to RIM Systems, this has often translated into increases in the quantity and connectedness of data added into the system. Prior to university adoption of this software, much of their data was spread across multiple internal and external platforms and potentially accessible only to those with access permissions. RIM Systems bring this data into a single system, interlinked and accessible to a wider range of people within and outside the university. Indeed, multiple individuals and groups within higher education institutions find clear advantages to having access to a single, authoritative source of institutional data pertaining to research activity. RIM Systems can save time and increase the accuracy of the many reports that are required for accreditation, academic program reviews, tenure and promotion, and grant reporting. It can help researchers, funders, and members of the public identify expertise within the university, and enable faculty members to communicate their research focus and activities more effectively. It can increase transparency, facilitate communication, and increase efficiency across the organization. For librarians, RIM Systems provide specific information on faculty research, the courses faculty are teaching, and the journals in which they are publishing (and therefore, with some additional work, the journals and books they are citing). This information can then be used as a factor in collection management and serials renewal/cancellation decisions, as well as library instruction and outreach efforts.

At the same time and for precisely the same reasons, there are considerable privacy implications for both individuals, groups, and the university as a whole that must be factored into in RIM Systems adoption, implementation and administration. The purpose of this case study is to describe and reflect upon the experience of Oklahoma State University in selecting and implementing a RIM System for our campus, focusing on conversations and decisions pertaining to privacy. After a brief review of the literature, we will outline the scope of the project to the present, describing the policies and considerations with reference to data

privacy, including user privacy controls, institutional privacy controls, API and reporting database access, and data modeling & privacy policies.

Literature

Privacy is number two (behind only Information Security Strategy) on Educause's "Top 10 IT Issues 2020", where they frame the issue in terms of balancing the protection of privacy with "providing easy and deep access to data across numerous systems, stakeholders, and compelling use cases."[4] They differentiate between "information security"—focused on protecting the confidentiality, integrity, and availability of data—versus privacy, which is centered on "the laws, practices, and norms about how information is collected, used, and disclosed."[5] However, it is clear the two are intertwined, as a breach in security can amount to a breach of privacy if the data is misappropriated. Privacy can be conceptually separated into "autonomy privacy," wherein one has the right to conduct their activities without being surveilled, and "information privacy," wherein one has a right to control the ways that their personal information is being used. Both of these categories are potentially impacted with the implementation of RIM Systems. Daniel Solove points out that when a large organization has "control over a vast dossier" of an individual's activity, the "routinized and sometimes careless way of handling information—with little to no accountability" can lead to important

---

[4] Susan Grojek and the 2019–2020 EDUCAUSE IT Issues Panel, *Top 10 IT Issues, 2020: The Drive to Digital Transformation Begins* (Educause, 2020), accessed July 1, 2020, https://er.educause.edu/articles/2020/1/top-10-it-issues-2020-the-drive-to-digital-transformation-begins.

[5] Educause Higher Education Information Security Council, "Privacy," in *Information Security Guide: Effective Practices and Solutions for Higher Education* (Educause, n.d.), accessed July 1, 2020, https://www.educause.edu/focus-areas-and-initiatives/policy-and-security/cybersecurity-program/resources/information-security-guide/privacy.

decisions being made that affect the individuals' lives "to which [they] are not always privy."[6] He continues, "certain uses of databases foster a state of powerlessness and vulnerability created by people's lack of any meaningful form of participation in the collection and use of their personal information."[7]

Furthermore, overreliance on quantitative and categorical information can lead to rankings and metrics that fail to account for critical qualitative and contextual information. Two predominant examples of this within higher education are the use of university rankings as proxies for quality of universities, and citation metrics to judge the performance of individual researchers. Here, criticism of "datafication" can extend beyond privacy into concerns about injustice, inequality, and exclusion. This includes charges that data "contributes to structural conditions that continue or create new injustices"[8] and can be "generative of new forms of power relations."[9] While analysis of these concerns is beyond the scope of the present case study, it is important to consider the larger context of data collection and use within higher education and society in general.

Christine Borgman coins the term *grey data* to refer to the "the vast array of data that universities accumulate outside the research realm;" that is, data generated by and about individuals "in their daily activities of research, teaching, learning, services, and

---

[6] Daniel J. Solove, *The Digital Person: Technology and Privacy in the Information Age*, (New York: NYU Press, 2004), 9, https://archive.org/details/isbn_9780814798461.

[7] Solove, *Digital Person*, 48.

[8] Lina Dencik, Fieke Jansen and Philippa Metcalfe, "A conceptual framework for approaching social justice in an age of datafication," DATAJUSTICE project, 2018, accessed July 1, 2020, https://datajusticeproject.net/2018/08/30/a-conceptual-framework-for-approaching-social-justice-in-an-age-of-datafication/.

[9] Ruppert, Evelyn, Engin Isin, and Didier Bigo. "Data Politics." *Big Data & Society*, (December 2017). doi:10.1177/2053951717717749.

administration."[10] Framing universities as "guardians of the public trust," she calls on them to be even more attentive to privacy considerations. Good data stewardship demands thinking through cases in which data should be made available for reuse, and those in which it should be securely protected or destroyed. "When the technologies are in the realm of ideas and knowledge production, as is the case with research and grey data," she writes, "the stakes for universities are especially high."[11] Though she cites teaching and learning data as the "primary exemplar" of *grey data*, she could have also pointed to data in RIM Systems.

The Directory of Research Information Systems (DRIS) is the largest database of institutional adoption of RIM Systems. Largely focused on universities in Europe and Asia, it reports 707 instances globally in operation, with an additional 21 in development.[12] Though a similar database or comprehensive survey for RIM System usage in American universities does not exist, a number of articles (and informal reviews by authors of the present study) attest anecdotally to the growth of such systems in the United States. However, despite this expansion, there is remarkably little research or analysis in either the peer-reviewed literature or the predominant higher education journalism examining RIM Systems adoption and use, let alone their privacy implications. A 2017 global survey administered by OCLC Research and euroCRIS, though employing a convenience sample and therefore intended to be exploratory rather than representative, is nevertheless the "largest and most comprehensive study ever conducted in the area of research information management practices."[13] Within the sample, RIM Systems adoption was "growing in countries without strong national reporting

---

[10] Christine L. Borgman, "Open Data, Grey Data, and Stewardship: Universities at the Privacy Frontier," *Berkeley Technology Law Journal* 33, no. 2 (April 2018): 366.

[11] Ibid., 395.

[12] Available at https://www.eurocris.org/dris.

[13] Bryant, et al. "Practices," 81.

mandates, driven by reasons other than compliance, such as improved decision support and improved researcher services."[14] However, this report does not include a question on privacy, nor does it include any instances of the word "privacy" within the document. In the dataset underlying the report, one respondent called for "guidance on agreements that libraries/universities sign with RIM vendors, to protect their interests (e.g., user privacy, data ownership)." Two other respondents—one from the United Kingdom and another from the European Union—referenced the need for RIM systems to align with national privacy legislation.[15]

The most in-depth and critical document with regard to RIM Systems and privacy is a report written by committees on the University of California Academic Senate, entitled "Concerns Regarding the Use of Research Information Management Systems."[16] Citing the "encroachment" of commercial parties into university operations and functions, the report authors point to the "significant threat these systems pose if not regulated by strong data governance," and call for the university to set policies on "data generated about faculty, addressing their ownership, collection and reuse and public-private partnerships." The authors further recommend that data created in RIM Systems should not be "resold to third

---

[14] Ibid., 83.

[15] Rebecca Bryant, Anna Clements, Pablo de Castro, Joanne Cantrell, Annette Dortmund, Jan Fransen, Peggy Gallagher, and Michele Mennielli, *Survey Instrument: Practices and Patterns in Research Information Management: Findings from a Global Survey* (Dublin, OH: OCLC Research, 2018), https://doi.org/10.25333/P9JT-W154.

[16] Maryann E. Martone, Schneider, Richard A., Swift, Allegra, and Mitchell, Catherine. *Concerns Regarding the Use of Research Information Management Systems at the University of California* (Oakland: University of California Academic Senate, 2019), accessed July 1, 2020, https://senate.universityofcalifornia.edu/_files/reports/rm-jn-mb-rims.pdf.

parties, at least without the consent of the university and subject to university governance policies."[17]

In their study on researcher uses of RIM Systems, Stvilia, Wu & Lee identified the primary reasons for faculty not having a public RIM System profile as: "not being required to have one, having no effect on their status, not being useful, or not being a norm in their fields." Concerns over privacy, in other words, were not identified as a significant issue.[18] Several existing case studies on RIM Systems focus on aspects other than privacy, such as integration with institutional repositories,[19] implementation to fulfill publications reporting needs,[20] motivations for engaging with RIM Systems,[21] and library roles.[22]

---

[17] Martone et al., *Concerns*, 10.

[18] Besiki Stvilia, Shuheng Wu, and Dong Joon Lee, "Researchers' Uses of and Disincentives for Sharing Their Research Identity Information in Research Information Management Systems," *Journal of the Association for Information Science and Technology 69, no. 8* (2018): 1044, doi: 10.1002/asi.24019.

[19] Jamie Wittenberg, "Putting the IR in RIMS: Towards an Automated Integration Between Institutional Repositories and Research Intelligence Systems," *Against the Grain* 31, no. 5 (2019), https://against-the-grain.com/2019/12/v315-putting-the-ir-in-rims-towards-an-automated-integration-between-institutional-repositories-and-research-intelligence-systems/.

[20] Alison D. Kissling and Kimberly D. Ballinger, "Implementation of a Research Information Management System in a Pediatric Hospital," *Medical Reference Services Quarterly* 37, no. 2 (2018): 184–197, doi: 10.1080/02763869.2018.1439224.

[21] Besiki Stvilia, Shuheng Wu, and Dong Joon Lee, "Researchers' Participation in and Motivations for Engaging with Research Information Management Systems," *PLOS ONE*, 2018, doi: 10.1371/journal.pone.0193459.

[22] Annette Day, "Research Information Management: How the Library Can Contribute to the Campus Conversation," New Review of Academic Librarianship, 2018, doi: 10.1080/13614533.2017.1333014; Marlee Givens, Lisa A Macklin, and Paolo Mangiafico, "Faculty Profile Systems: New Services and Roles for Libraries," 2017, doi: 10.1353/pla.2017.0014.

OSU RIM System Procurement

The Oklahoma State University Library began exploring RIM Systems beginning in 2017 as a response to needs expressed by multiple university parties for a single, authoritative source of institutional data pertaining to faculty research. Both faculty and university administration saw such a resource as useful for increasing the accuracy of information and decreasing the time spent compiling reports. In addition, a number of faculty members called for a more systematic way of exploring and identifying expertise and research focus of their colleagues on campus. Since roughly the mid 2010s, libraries have increasingly taken a leading role in RIM System implementation and administration (Bryant et al., 2017; Day, 2018; Givens et al., 2017). Librarians bring proficiency with publications metadata and a deep understanding of the databases from which the metadata is harvested by RIM Systems. We also have experience with data modelling and developing crosswalks between schemas, which is essential as the RIM System requires mapping data from multiple different databases. In addition, libraries work with vendors, maintain database platforms, manage large projects, and cultivate relationships with individuals and departments across campus.

After several months, conference calls, presentations, meetings, emails, more meetings, and more emails, we selected Symplectic Elements in Fall 2019. During the exploratory phase, questions about user privacy and data ownership were at the forefront of our investigation of various RIM Systems. From the library's perspective, our ideal preference would have been to use open source tools and host all data locally; however, we are a small team with multiple obligations and no software developers, and this option was

not feasible. With reference to the Scholarly Communications Infrastructure Checklist[23] and the recommendations of the *SPARC Landscape Analysis*[24] we developed a set of questions related to privacy, information security, and data ownership:

- Please provide information regarding data protection policies and practices.
- How do you reuse user information? Do you share it with the client institution? Do you share it with the user? Do you share it with your business partners?
- If we stop subscribing to your product, what data will the vendor keep?
- How do you use the data that is harvested and inputted into your system?
- Is our data shared with any of your other services? Is our data shared with any third-parties? Is our data monetized in any way? Will our data ever be sold back to us?
- What control do we retain over what can be done with the data generated by our use of this system?
- What controls do individual users have over the ways that other users in the system can view and access the data they input?
- Who owns the data generated by the use of this product? Does the vendor assert ownership over any data generated by users?
- What happens to a user profile and associated data when a user separates from OSU?

These questions revolve predominantly around the vendor's policies and practices as they relate to information privacy--that is, the right to control how data is reused. The

---

[23] Elena Feinstein, Emily Frank, Vanessa Gabler, Robyn Hall, Claudia Holland, Allison Langham-Putrow, David Minor, Charlotte Roh, and Allegra Swift, *Scholarly Communications Infrastructure Checklist* (2018), doi: 10.6084/m9.figshare.7406849.

[24] Claudio Aspesi, et al., *SPARC Landscape Analysis* (Washington, DC: SPARC), 2019, doi: 10.31229/osf.io/58yhb.

contract was reviewed by multiple stakeholders across the university, including faculty, IT, administration, and the library. Though the vendor offered the option to host the RIM System on our local servers, we opted to contract with them to host it after our IT team received satisfactory answers to questions they had pertaining to security. We sought contractual assurance that the vendor did not claim ownership over any information that OSU faculty and staff added to the RIM System. Indeed, the vendor we contracted with specified that nothing in the contract operates to transfer to them intellectual property ownership in any data that members of our university add to the system. The contract further stipulated that the vendor would not provide our data to third parties without our permission, and that our data would be destroyed upon termination of the agreement. In addition, as explored below, the system included individual user privacy controls, allowing them some choice in ways their data is accessible and displayed.

OSU RIM System Implementation

Following procurement, an implementation team formed, comprising librarians, IT, Human Resources, Associate Deans, faculty members, grants staff, registrar staff, and others. The team held discussions about the system with OSU Faculty Council, administrators, department heads in all colleges, and several others with interest in the project. The user profiles were established (see below, "Institutional Privacy Controls"), the publications harvesters were configured, and the process for mapping OSU data for grants and courses to the Elements data structure began. The team has worked closely with Associate Deans for Research, department heads, and individual faculty members to develop customized data types reflective of their work and contributions. As of Summer 2020, the library has provided training to users in several colleges, and the system is moving towards fully operational. At

this stage, the RIM System is internal--that is, accessible to specified OSU users only--however, public faculty profiles will be generated from the RIM System in 2020-2021.

Despite the public nature of much of the data that is automatically imported into the system, and the out-of-the-box setup and services, OSU's RIM System brought to the fore several aspects of implementation that impact privacy, particularly decision-making around user privacy controls, institutional privacy controls, API and reporting database access, and data modeling. In some cases, our decisions were constrained by the affordances of the platform; in others we made decisions with reference to relevant institutional policies, consultation with the implementation team, and/or discussion with other institutions with RIM Systems.

User Privacy Controls

RIM System Users

Faculty are both the primary users of the RIM System and the primary data providers. Additionally, administrators, who are also often faculty, utilize or will utilize this information for reporting across the institution, for external reporting, and for annual and promotion and tenure reporting. While many other institutions include graduate students as users with profiles in their systems, in the initial rollout OSU elected to exclude student profiles, out of scope of the implementation goal to elevate faculty research. As will be discussed below, despite the lack of student users it was still necessary to take the Family Educational Rights and Privacy Act of 1974 (FERPA) into consideration as the system was developed.

User Profile Privacy

Anecdotally, in almost every training session first-time faculty users ask if they are able to hide certain information from view. Users have several options to control the privacy of their

own data. In this sense they have some control over who is able to publicly or internally view their researcher profile at several points in the data configuration process: 1. Researchers can exclude their entire profile from view. 2. They can choose to hide specific components of their profile, such as individual publications, from view by marking them private one by one. 3. They can opt to be excluded from the system.

When a user edits their profile, the current profile privacy setting is highly visible at the top of the page with a link to "Learn More." This takes the user to a ready-made page explaining the privacy settings within the RIM System, although it does not include methods for opting out entirely or links to the privacy policies of the RIM System vendor or linked systems. A configurable privacy statement area appears at the bottom of the page with default text to contact the system administrator. In this space, OSU Libraries created a basic local support web page on privacy matters that includes OSU's general privacy statement, links to privacy policies for integrated systems, and steps showing how to configure privacy settings.[25]

Users may choose from three levels of privacy, public, internal, and private, for the overall researcher profile as well as specific components of their profiles:

- Public: When OSU develops a public profile website, this data will be publicly available.
- Internal: Only other users can see this data.

[25]"Experts Directory and Privacy - Experts Directory - Guides at Oklahoma State University-Stillwater," accessed July 1, 2020, https://info.library.okstate.edu/experts/privacy.

- Private: This information is visible to the user, the user's delegates and administrators.

Setting a researcher profile to public will display on the public-facing website only the data selected for inclusion by system administrators and only the components not marked as private. Although internal profiles do not appear on the public-facing website, they are visible to all other users within the RIM System. Private data is still viewable by system administrators, institutional administrators with reporting access, and delegates. The internal and private settings are useful for publications or projects that are in progress or otherwise not ready to be shared with colleagues or the public. For example, a faculty member may wish to include a grant applied for but not awarded in their annual or promotion and tenure review, but prefer to exclude the application from public or internal view.

University administrators and many faculty consider this ability to share personal data publicly an incredibly useful service. A RIM System provides a single authoritative profile within the university domain, a clear improvement over the myriad, free profile systems available around the web. In training sessions, early adopters or "Power Users" expressed excitement about the system. An important difference between previous iterations of faculty profile systems and websites and a RIM System, however, is that the traditional directory or CV data now appears alongside altmetrics and journal impact metrics that quantify faculty output at a glance. Faculty in vastly different fields of study with different publishing timelines, publication expectations and definitions of research--for example, high-energy physics and graphic design--are now part of a single snapshot of institutional research captured with uniform metrics. Despite significant research and international proclamations questioning the validity of tying bibliometric indicators to performance, these metrics continue to play a key role in tenure and promotion decisions; thus their inclusion in the

system is not entirely unproblematic. This relatively new collation of data from a vast array of previously disassociated, obscure sources, including social media, may present privacy concerns. A recent study by Aung et al. found, "Lack of privacy is also a concern for scholars when using altmetrics. This was found in the literature review (Stutzman et al., 2011) as well as in our survey results....Only 2% of the participants said that traditional metrics lacked privacy, but 14% of the participants felt altmetrics lacked privacy." As more faculty see their research profile visualized alongside their peers in the RIM System for the first time additional concerns around privacy may arise that prompt a more nuanced or localized approach to research profile data.

Institutional Privacy Controls

OSU populates its RIM System user profiles through automated collection of Human Resources data stored in the University's Human Capital Management (HCM) software. A csv file with directory data is generated from the HCM system and uploaded nightly into the RIM System. The OSU implementation pulls all faculty employed by OSU from a certain point in time and flags them as active or inactive. Those users remain in the system indefinitely, although inactive users will have limited data associated with their profile, which remains out of the view of both general users and the public. For active users or soon-to-be inactive users, it is not possible to opt out or to remove a profile from within the RIM System. As noted above, it is also not possible to have a completely private profile. Some users with greater privileges are able to view all users within their user group, including any hidden parts of their profiles. A user would need to work directly with Human Resources to flag themselves in the HCM System in order to opt out from the RIM System entirely. Opting out would require that alternate provisions be made for annual reporting as well as for filing annual review and promotion and tenure documentation.

Within the RIM System system administrators may configure system-wide settings that impact user privacy. OSU has procured and rolled out the system with the intention of creating public profiles. This is documented in training materials and widely shared with users. Since OSU is still in the process of implementing a public system, all profiles are currently internal with the intention to make all profiles public at some point, either all at once when the public system goes live or in stages by college or by profile completeness. A report is available for "profile completeness" that may help prevent the publicizing of incomplete profiles--for instance, absence of photos, degree and appointment information, publication and service activity, etc. Additional system-wide settings include visibility of email addresses, whether the user may override these settings, and whether the institution will utilize third-party altmetrics or analytics tools such as Google Analytics.

As is common in other management systems, users are assigned a level of access as part of a group and also as individuals where indicated. During the pilot phase, the library implementation team relied on input from the Associate Deans of Research and department heads of each college to identify users who should be given additional privileges for reporting, system administration, or administrative support. This led to conversations clarifying the variety of access levels and asking critical questions about how to achieve a usable amount of data while maintaining the privacy of their faculty users. Including the RIM System in OSU's existing access request procedure for IT applications helps ensure compliance with various university policies governing data access.[26]

---

[26] For instance, the OSU Human Resource Information Management Systems policy, available at https://adminfinance.okstate.edu/site-files/documents/policies/human-resources-information-management-systems.pdf, and the OSU Data Stewardship policy, available at https://adminfinance.okstate.edu/site-files/documents/policies/data-stewardship-data-classification-policy-responsibilities-and-guidelines.pdf.

To supplement the built-in system roles, OSU adopted a "power user" support model, which sets up faculty users and administrative staff as a support network of early adopters available to their peers using the system.[27] This model both extends the limited support the library is able to provide and helps shape user support to the unique requirements of each college. Power users are often department heads, department administrative assistants, and college administrators, but are also self-identified individual faculty members. Depending on the needs of the college, power users may also help with the initial push to input CV data in the system for all users in their departmental group or rejecting and accepting publications imported from linked systems such as Scopus.

Initially we intended to permit all power users to manage other users' profiles through the "impersonation" feature. Impersonation is a key feature that allows a delegate or other privileged user to edit another user's profile data. On one hand, this permits an administrative assistant, for example, to quickly and easily manually enter publications data on behalf of a faculty member, and increases the likelihood of adoption and usable data for the institution. On the other hand, it could potentially result in misuse or an undesirable dynamic within an academic department. This observation resulted in a finer gradation of system privileges, relying on the delegation option for users to provide access to their profile to power users or others at their own discretion. Those administrative support staff tasked by administration to complete profiles were assigned the system role that allows them to impersonate users in order to input data on behalf of faculty.

[27] The inspiration for this model and terminology came from the Scholars@Duke RIM System developed at Duke University, available at https://about.scholars.duke.edu/locate-power-user.

API and Reporting Database Access

The system role granting the ability to run reports without modifying user profile data was also frequently applied. The OSU RIM System contains research data useful to many stakeholders across campus. These include the Institutional Research and Analytics office responsible for gathering statistics on university activity, including faculty output, for everything from accreditation to rankings. Access to the data can be gathered by API or the SQL-based reporting database. Unique accounts separate from the user profile system and IP address limit access. These accounts are configurable only by system administrators. The RIM System defines API access to HR data and annual/tenure review data separately with write access as an additional privilege. It is not possible to limit API access to a particular user group, for example, so that the IT manager of a particular college may only access data from that college. Setting up access to this data through the University access request procedure for IT applications, again provides a level of security and consistent implementation of policy that is beyond the scope of the library and more efficiently handled centrally.

Data Structure Modifications

RIM Systems primarily focus on collecting research publication data, but they also include an avenue for annual reporting on all aspects of faculty professional activity, including teaching, grants, service, and other professional activities, typically outside of the realm of libraries. As mentioned previously, OSU elected not to include graduate student profiles in the RIM System. Opportunities remain, however, for student data and other sensitive information to enter the system. Customizing the data structure is one way to exclude unnecessary, possibly sensitive data not required for reporting. OSU's RIM System included a built-in checkbox for identifying students who had given permission to have their name used in an activity record.

Since this checkbox does not fit squarely with FERPA recordkeeping at OSU, we removed fields, such as student identifier and student name, from the activity record when it was not necessary for reporting or did not meet the criteria for FERPA directory information. We are exploring options for automating advisor data entry in order to ensure exclusion of students with Buckley flags who have opted out of sharing their directory information. Without automatic import, this data must be cross-checked manually in the Learning Management System and leaves room for faculty erroneously adding student advisees with a Buckley flag to their faculty profiles.

When data is entered that later needs to be deleted, privacy concerns may arise. Some data once entered is difficult to delete; it instead remains associated with the profile as "rejected." This may be data automatically collected from university systems or self-populated. For example, a publication that is automatically collected from a linked publications database and incorrectly associated with a person is rejected rather than deleted from a profile. It retains its association with the user so that the user is not repeatedly asked to claim the same article. This is also the case for a manually recorded publication. It can be rejected but not deleted later, although the data record can sometimes be repurposed by manually overwriting it with new data. The best option for keeping data truly private is to not include it in the system.

As is often the case, once previously hidden data is migrated into a discovery system errors become much more apparent. For example, while many grants are a matter of public record, faculty may wish to keep grants from partners in industry or in sensitive research areas private. In OSU's system, these records may be hidden from general view by the user profile privacy methods listed above, although they will still be visible to administrators. If additional privacy is required, data ported from another system needs to be queried in order to exclude sensitive records from import into the RIM System. OSU identifies appropriate

contacts for editing or removing data (often from the Human Capital Management System) on our support page. Once data is in the system, it is available to the vendor and third parties for data analytics purposes, and although de-identified, depending on the specific nature of the research, may be possible to re-associate with a particular researcher, even after a record is rejected.

Privacy Policies

Users or librarians wanting to know more about RIM System vendors' privacy policies may find them at Privacy Shield, an international organization that helps ensure international data security compliance for companies.[28] While each company provides its own data assessment, and the policies pertain mostly to user-supplied or anonymized data it does provide a clearer picture of a company's subsidiaries and some third-party integrations for further research. Listings of open-source and research aggregator integrations in OSU's RIM System were discovered elsewhere, such as the attribution section of the internal help page and data source management page. Of the third-party integrations in OSU's RIM System, ORCID provides the most comprehensive privacy policy.[29] It is a lesson in basic privacy issues ranging from data reuse and retention to cookies in web browsers. Walking users through the ORCID profile process provides another opportunity to educate users about privacy issues around research data. For example, in order to integrate their profile with the RIM System, an ORCID user must explicitly give ORCID permission to both read and write to the RIM System profile. Additionally, clear levels of visibility such as "Everyone data," "Trusted

---

[28] "Privacy Shield," accessed July 1, 2020, https://www.privacyshield.gov/welcome.

[29] "ORCID Privacy Policy," March 31, 2020, https://orcid.org/privacy-policy. Although not mandated to comply as a nonprofit organization, ORCID participates in Privacy Shield.

data," and "Only me" show how data at each level of visibility is repurposed. There is also an opt-out tool for cookie use by third parties for interest-based ads.[30] While not directed specifically toward RIM Systems, the DLF Privacy and Ethics in Technology Working Group's Glossary is an excellent starting place for exploring privacy terminology and issues in the library.[31]

Conclusions

As RIM Systems are beyond their infancy, and are operational in thousands of universities around the world, there is a significant need for deeper engagement in the scholarly literature with the issues they engender, such as privacy. While user communities have coalesced around specific RIM Systems and can serve as a resource for these questions, there is need for a more formal organization in North America, as suggested by Scherer, et al., to provide recommendations, documentation, use cases, and best practices.32 Other important considerations still in deliberation include, for instance:

- Do users who wish to opt out of the system altogether have that option? As addressed above, while it is technically simple to remove a user from the feed, there are policy

[30] "WebChoices: Digital Advertising Alliance's Consumer Choice Tool for Web US," accessed July 1, 2020, https://optout.aboutads.info/?c=2&lang=EN.

[31] Andrew Asher et al., "Ethics in Research Use of Library Patron Data: Glossary and Explainer," October 2, 2018, https://doi.org/10.17605/OSF.IO/XFKZ6. See also *Privacy in Practice: Applying the Tools & Resources of the Privacy & Ethics in Tech. Working Group*, accessed June 16, 2020, https://www.youtube.com/watch?v=UyFETAgPSx0&feature=youtu.be.

[32] Scherer, et al., *Comparison*.

and procedural considerations at play. How do we balance respect for privacy rights with the many complex reporting demands of the contemporary university?

- What if the organization is acquired by an entity that institutes policies that challenge your institution's values and/or policies? In the realm of privacy, this issue was recently raised with the sale of a popular learning analytics platform and concern over the ethical handling of student data transferred with the sale.[33] This concern is addressed in the *SPARC Landscape Analysis*; if developing an in-house solution or deploying an open source tool is not possible, the authors recommend risk mitigation strategies; for instance, demanding ownership of the data is not transferred or resold to third parties, that contracts are not covered by non-disclosure agreements, and that universities "identify individuals tasked with both issuing data policies, monitoring execution, and helping individual offices negotiate with vendors and adjudicate possible conflicts of interest across different parts of the institution."[34]
- To what extent does usage of a RIM System reinforce a culture of metricization, managerialism, datafication, and productivity as a proxy for quality? This is a privacy issue inasmuch as it can have a direct effect on the individual's research and service activities. The answer is partly dependent upon the configurability of the system (i.e. whether it allows for data inputs reflective of the diversity of work that faculty engage in) as well as the ways in which the system is used. Alternatively, a RIM System can

[33] Jeffrey R. Young, "As Instructure Changes Ownership, Academics Worry Whether Student Data Will Be Protected," *EdSurge*, January 17, 2020, accessed July 1, 2020, https://www.edsurge.com/news/2020-01-17-as-instructure-changes-ownership-academics-worry-whether-student-data-will-be-protected.

[34] Aspesi, *SPARC*, 53.

be empowering if it is used to "support the ability of faculty/colleges to craft rich narratives of the significance and impact of their work."[35]

This case study presents practical considerations and outstanding questions for addressing privacy concerns in RIM Systems with the hope of stimulating a larger discussion of how researchers can take an active role in the representation of their own "rich narratives" in Research Information Management Systems.

[35] Bruce E. Herbert, Dong Joon Lee, Doug Hahn, and Ethel Mejia, "Using Campus Needs Involving Tenure & Promotion, Interdisciplinary Collaborations, and Institutional Research to Drive the Evolution of VIVO at Texas A&M University," (College Station, TX: OAKTrust), 2019, http://hdl.handle.net/1969.1/177789.

Bibliography

Borgman, Christine L. “Open Data, Grey Data, and Stewardship: Universities at the Privacy Frontier.” *Berkeley Technology Law Journal* 33, no. 2 (April 2018): 365–412.

Bryant, Rebecca, Anna Clements, Pablo de Castro, Joanne Cantrell, Annette Dortmund, Jan Fransen, Peggy Gallagher, and Michele Mennielli. Practices and Patterns in Research Information Management: Findings from a Global Survey. Dublin, OH: OCLC Research, 2018. https://doi.org/10.25333/BGFG-D241

Bryant, Rebecca, Anna Clements, Pablo de Castro, Joanne Cantrell, Annette Dortmund, Jan Fransen, Peggy Gallagher, and Michele Mennielli. Survey Instrument: Practices and Patterns in Research Information Management: Findings from a Global Survey. Dublin, OH: OCLC Research. https://doi.org/10.25333/P9JT-W154

Educause Higher Education Information Security Council. “Privacy.” In *Information Security Guide: Effective Practices and Solutions for Higher Education*. Educause, **2020??**, https://www.educause.edu/focus-areas-and-initiatives/policy-and-security/cybersecurity-program/resources/information-security-guide/privacy.

Feinstein, Elena, Emily Frank, Vanessa Gabler, Robyn Hall, Claudia Holland, Allison Langham-Putrow, David Minor, Charlotte Roh, and Allegra Swift. *Scholarly Communications Infrastructure Checklist.* 2018, https://doi.org/10.6084/m9.figshare.7406849.

Grojek, Susan and the 2019–2020 EDUCAUSE IT Issues Panel. “Top 10 IT Issues, 2020: The Drive to Digital Transformation Begins.” Educause. Accessed June 30, 2020. https://er.educause.edu/articles/2020/1/top-10-it-issues-2020-the-drive-to-digital-transformation-begins.

Herbert, Bruce E.; Lee, Dong Joon; Hahn, Doug; Mejia, Ethel. “Using Campus Needs Involving Tenure & Promotion, Interdisciplinary Collaborations, and Institutional Research to Drive the Evolution of VIVO at Texas A&M University.” College Station, TX: OAKTrust, 2019. http://hdl.handle.net/1969.1/177789.

Kissling, Alison D, and Kimberly D Ballinger. “Implementation of a Research Information Management System in a Pediatric Hospital.” Medical Reference Services Quarterly 37, no. 2 (2018): 184–197.

Martone, Maryann E., Schneider, Richard A., Swift, Allegra, and Mitchell, Catherine. *Concerns Regarding the Use of Research Information Management Systems at the*

University of California. Oakland: University of California Academic Senate, 2019. https://senate.universityofcalifornia.edu/_files/reports/rm-jn-mb-rims.pdf.

Scherer, David, Kate Byrne, Mark Hahnel, and Daniel Valen. “Collaborative Approaches to Integrate Repositories within the Research Information Ecosystem: Creating Bridges for Common Goals.” The Serials Librarian 78, no. 1–4 (June 1, 2020): 181–90. https://doi.org/10.1080/0361526X.2020.1728169.

Solove, Daniel J. 2004. *The Digital Person: Technology and Privacy in the Information Age*. New York: NYU Press, 2004, https://archive.org/details/isbn_9780814798461.

Stvilia, Besiki, Shuheng Wu, and Dong Joon Lee. "Researchers' uses of and disincentives for sharing their research identity information in research information management systems." *Journal of the Association for Information Science and Technology* 69, no. 8 (2018): 1035-1045.

Stvilia, Besiki, Shuheng Wu, and Dong Joon Lee. “Researchers’ Participation in and Motivations for Engaging with Research Information Management Systems.” *PLOS ONE*, 2018. https://doi.org/10.1371/journal.pone.0193459.

Wittenberg, Jamie. “Putting the IR in RIMS: Towards an Automated Integration Between Institutional Repositories and Research Intelligence Systems.” *Against the Grain* 31, no. 5 (2019). https://against-the-grain.com/2019/12/v315-putting-the-ir-in-rims-towards-an-automated-integration-between-institutional-repositories-and-research-intelligence-systems/.