WESTUDIO/SHUTTERSTOCK.COM

Responsible Collection, Use, and Disclosure of Data: Considerations for Building Enclosure Professionals

By Margaret H. McKay, MSc, JD, PMP, CIPP/C, and Alana Gin, Dip. Eng.

Disclaimer

This paper is intended as a high-level consideration of ethical factors relating to data. Nothing herein constitutes legal or professional standards advice. Laws and requirements vary widely between fields and jurisdictions. Those with specific questions should seek local expert advice.

With the recent attention to social media and artificial intelligence (AI), one might think that ethical challenges related to data are new. Regrettably, they are not.

Building enclosure professionals collect, use, and share a range of data in their work. This includes specifications, standards, measurements, and observations, as well as recommendations and best practices. Every aspect of decision-making in relation to data—from decisions on what to collect to how to use it and what to disclose to whom—can trigger considerations of responsible data and professional ethics.

"Responsible data" is used to describe the range of considerations pertaining to decisions about what data and information to collect and how to use and disclose it (see sidebar, "Data and Information"). For decades, governments and organizations have tried to define core requirements for the treatment of data. Management Information Systems experts wrestled with ethical considerations, including how to address questions of accuracy and property in data, in the 1980s,[1] laying the groundwork for questions faced by professionals who rely on data today.

Modern formal efforts to provide guidance are widely seen as having begun when the United States government developed Fair Information Principles in the 1970s.[2] Internationally, this was followed by the development of guidelines containing eight related principles by the Organization for Economic Co-operation and Development (OECD Guidelines).[3,4] These principles, while focused on information about identifiable individuals, can also be seen as a useful framework to assess the responsible use of important data in a range of less personal contexts. This article draws on the eight principles within the OECD Guidelines to inform a discussion of considerations in the collection, use, and disclosure of data and information (collectively, "responsible data") for building envelop professionals.

Data and Information

It is possible to distinguish between "data" and "information." However, in the context of responsibility and ethics, this is rarely necessary or helpful. Formal efforts to codify expectations in this area largely began with a focus on "information," and specifically "personal information." These efforts expanded to include data as large-scale data processing became more common. While definitions vary, "data" tends to be used to refer to initial observations, readings, and the like, and "information" refers to the results of data processing, providing broader statements of condition, status, and causation among others. Thus, one can envision a spectrum with "data" on one end and "knowledge" on the other, and information bridging the two. Professionals should focus on how they handle this material irrespective of whether it is referred to as "data" or "information." For brevity, the text of this article typically refers to either data or information depending on context; however, both should be considered.

Every profession and context has its own data challenges. The "Principles of Responsible Data" section of this article provides key elements for consideration; and the "Data Accountability on the Job" section explores some specific contexts of potential relevance to the work of building enclosure professionals. Various professional and regulatory bodies will also have their own requirements. Additionally, there is a host of laws, standards, and regulations to consider depending on the location and the job. This article takes a higher-level perspective, looking at ethics rather than specific professional or jurisdictional requirements.

PRINCIPLES OF RESPONSIBLE DATA

The eight core principles within the OECD Guidelines[3] are: collection limitation, data quality, purpose specification, use limitation, security safeguards, openness, individual participation, and accountability. When considered in the context of technical work, these eight principles can be organized into five areas familiar to building enclosure professionals:

Plan the Work and Work the Plan

The core principles included in this section are purpose specification, collection limitation, and use limitation. "Purpose specification" means that there needs to be a known and articulated reason to collect information before the data collection starts. This reduces "fishing expeditions" and helps to ensure that all the data needed for a particular purpose can be collected.

The requirement to limit the collection and use of data to the original purpose serves this same objective. It demands a clear plan and, in the event of a change to the reason for investigation or a need for additional data, a new plan should be developed and communicated to all affected. In some cases, limiting data collection can also help to reduce scope creep and potential issues related to personal information.

In most cases, personal information of third parties will not be necessary to a building enclosure professional's work and should not be collected. Building enclosure professionals may generate and gather data in a range of ways that do not involve third parties. However, in some cases, the professional may encounter personal information, for example through sensor readings or via entry into tenant units, which hint at resident activities. If a client (for example, a landlord) asks the professional to report back on observations unrelated to their normal role (for example, on the presence of guests or pets in a rental unit), this should be discussed to avoid any risk of misrepresentation. In addition to the potential danger to the professional's reputation and professional standards, it is necessary to consider whether such out-of-scope activities are authorized by the agreements allowing the professional to enter the property.

Observing Professional Standards in Data Accuracy and Timeliness

The need for suitable data speaks for itself. While absolute perfection may not be required, any data or information that is relied on for a decision should be relevant to the question being investigated. Data should also be as accurate, complete, and as up to date as needed to responsibly conduct the study.

Maintaining Confidentiality

Professionals owe a duty to their clients and those whose property they enter to adequately protect the confidentiality and integrity of the data and information they receive in the performance of their duties. It is also important to consider what else may be learned from entering someone else's space.

Generally, data not relevant to the project should not be written down, retained, or shared with others. However, sometimes sensitive but irrelevant information may be acquired incidentally, for example in the background of technically relevant photographs or as context to how damage arose. Irrelevant and potentially sensitive data elements should be removed from any materials shared with the client or others in all contexts other than when specifically required in legal proceedings.

Data with the potential to help reveal information of personal, professional, or financial significance to clients, sites, or third parties, or which could be critical to the professional's report should be maintained in a secure location for as long as necessary to address not only the contract itself but potential follow-on issues or challenges. Security will sometimes mean more than just virus protection, up-to-date operating systems, and a password protecting the computer that has access to the files.

All internet-connected devices should be secured with strong passwords and updated regularly, even if they are only cameras or measuring devices. The use of a reputable virtual privacy network on cellphones and other devices should be considered when using public or unsecured Wi-Fi networks. It is important to match the stringency of protection, monitoring, and backups with the risk of harm if the information is altered, removed, or disclosed. For systems with multiple users, it is also advisable to have the ability to generate a log of who has accessed the information and what changes they may have made.

Professionals using paper to record sensitive and general data should have a system to keep the data safe. This could mean keeping the documents in a secure, fire- and water-resistant, and access-controlled filing cabinet and properly destroying the papers after digitization.

Obtaining Local Context and Perspectives

Personal Information

The principle of openness asks that professionals holding data of potential personal, professional, or financial significance to clients, sites, or third parties should be prepared to respond completely and honestly when those with a legitimate interest ask what data relevant to them the professional holds, where it is stored, and the purpose for which they are holding it.

It is important for professionals to consider privacy principles in all stages of their work. This means minimizing the amount of personal information collected during the work and avoiding the unnecessary disclosure of personal information in the course of the work and subsequent reporting. Different jurisdictions may define "personal information" differently. However, many definitions of personal information include what one would generally consider to be "data," which, alone or together with other data, could reveal something about a potentially identifiable individual. Best practices and some legislation require that those holding personal information about individuals provide the individual with a copy of that information upon request and a chance to correct provable errors.

Technical Information

In technical work, the principle of openness includes ensuring full context and considering alternative interpretations and understandings offered by those with day-to-day experience of the situation. There will be times when it is useful for professionals to permit those most familiar with the site or material under study to see related observations and measurements, and possibly the conclusions drawn from them, in order to offer comments and to identify possible errors. Although this will not be appropriate in all situations, there will be times when it can add context and bring value. As a best practice in appropriate circumstances, openness can help to improve the accuracy, suitability, and contextualization of data; identify areas of disagreement early; and build buy-in for the next steps following the report.

Accountability

Accountability, a defining characteristic of professionalism, will be very familiar to building

enclosure professionals. Professionals expect to be held to account for their actions and decisions regarding data or other aspects of their work. Generic professional accountability is reflected in practices such as standing behind professional assessments; proactively disclosing and avoiding potential, apparent, or real conflicts of interest; and being transparent about the limits of one's expertise. Accountability in a data context also raises further considerations of how data are collected, the transparency of the tools and methods used, and decisions to reuse or share parts of the data in the future. These are explored further in the next section.

DATA ACCOUNTABILITY ON THE JOB

A professional may encounter many kinds of data in a day, including specifications, standards, measurements, and observations, as well as recommendations and best practices. This section explores some examples of how accountability and other principles discussed in the previous section give rise to transparency; safety; and, reuse considerations, which can impact decisions about data. These considerations involve not only the content of an assessment but the manner in which it is packaged and presented, including:

Transparency

Transparency relates to the assessment approach, identifying areas of professional judgment, and the question addressed. Transparency of this type helps to support the principles of data quality, collection limitation, openness, individual participation, use limitation, and accountability.

Assessment Approach

When there is more than one potential assessment approach or rating system and a different approach would likely impact the assessment, it is important to be clear about the choice made and why it was appropriate.

Identifying Areas of Professional Judgment

Unless an instrument directly provides a value, there is some element of subjectivity in scoring the condition or nature of an observed site. This is part of the professional judgment for which clients pay. Be clear how the values were obtained. Any subjective (professional judgment) element to an assessment should be disclosed and contextualized in the findings.

The Question Addressed

Reports and any records intended to endure beyond the completion of the job should state the purpose for which the assessment was made and at whose request. It is important to state the perspective from which the assessment was made. For example, was the professional asked to assess whether observed water infiltration could have originated from a membrane failure; or, to assess what the source of water infiltration was?

Safety

When an inspection reveals a safety issue, applicable legal, professional, regulatory, and contractual requirements may specify when and to whom the risk must be reported. Some jurisdictions place a "duty to warn" on professionals in relation to serious risks to third parties. Professionals should be careful to know the applicable requirements and to ensure that their own contracts for service will support them in meeting their professional and legal obligations. In the event that repeated inspections and reports show that no action has been taken by the building owner or manager to resolve the same safety issue, all available steps to resolve the issue should be taken.

From an ethical perspective, professionals may wish to ensure that their standard contracts provide them the ability to report life-threatening situations to public authorities even in the absence of a legal or regulatory requirement. Local legislation and regulations, legal advice, and the applicable professional organization's ethics committee should guide the professional's actions.

Steps to clarify potential safety-related questions of this type will also help to support the principles of individual participation and accountability.

Reuse and Other Considerations

Choice by Professional to Reuse

Files accumulated over the years may be a goldmine of competitive intelligence about different kinds of products, builders, and sites. While the information found in old files could be useful to reduce future problems and improve efficiency, one must keep in mind potential legal, business, and contractual requirements. Under some circumstances, consent from each data source might be required prior to sharing information or using it in research. If a file contains data about people other than the client (for example, tenant data), additional factors beyond the professional service contract may be important. Those interested in using existing files for research should first seek legal advice.

Those interested in collecting data for future research use or to train future AI tools should ensure that their contracts for service will provide them with the necessary rights, and they should also familiarize themselves with data and metadata expectations in the field. Each context will have its own precise requirements. In broad terms, good research data management practices begin with ensuring that the data meets minimum standards for findability, accessibility, interoperability, and reusability.[5] These requirements facilitate appropriate use of the data by those who were not involved in its collection and who may seek to use it in ways which were not originally contemplated. Additionally, AI tools can be sensitive to bias in the data used to train them. Given this, any data intended for possible use in training AI should be well described and documented to enable future users to identify and address potential sources of bias.

Data Leakage from Inspection Apps and Cloud Services

A range of cloud-based services and applications exist to assist those involved in building inspection and assessment. While some of these tools do not appear to mine or otherwise reuse the data submitted by professionals, it appears that some may (see sidebar, "Data Privacy").

Data Privacy

As of the date of writing, some inspection apps reserve the right to share photos, videos, and other information related to inspections that is gathered by or stored in the app. Some other apps provide such limited information regarding their data practices that it is impossible to determine if data will be further used or shared. It is necessary for many apps to collect a certain amount of information in order to be useful to their user-clients.

However, with the exception of those apps designed to facilitate the submission of reports to third parties, there will generally be no need for an app to use or share inspection-related information aside from user-initiated requests. See, for example, the "data safety" section of app listings in the Google Play store. Examples of possible interest as of the date of writing include: "Property Inspect" by RadWeb; "InspectMe" by PropertyMe; "Home Inspection" by Spectora; and "Express Property Inspection" by OnSourceOnline. App terms of service and privacy policies may be updated frequently and often without notice.

Professionals have a choice in the tools they use and in how they disclose that use to their clients. Both data security and confidentiality should be considered from the perspectives of various stakeholders, including building owners and occupiers. Inspections may involve data relevant to a wide range of individuals, many of whom will have ethical or legal interests in how data are protected and shared.

Professionals should take the time to read the terms of service and privacy policies for the tools and services they use in their work, and to get clarification of any uncertainties, including any updates that may occur. If the company behind a tool uses inspection-related data for its internal research purposes or shares that data externally the professional should address this. Typically, the professional will have three options:

- use a different tool;
- disclose the use of the tool and the potential data implications to clients as part of the contract for service; or,
- continue to use the tool but do not input, capture, or otherwise share any information which, alone or together with other available information, might reveal any confidential or personal information.

While absolute perfection may not be required, any data or information which is relied on for a decision should be relevant to the question being investigated.

These steps help to support the principles of use limitation, security safeguards, openness, data quality, individual participation, and accountability.

CONCLUSIONS

The building enclosure industry is not immune to questions of data ethics and responsible use of data. However, principles such as those reflected in the OECD Guidelines,[3] together with relevant professional and regulatory requirements can provide a clear path forward for professionals.

The considerations discussed in this article are intended as a possible supplement to current professional standards and guidelines. Every context is different, and these considerations provide one useful perspective. Some of these factors are legal in nature. Given variability between jurisdictions, professionals should seek local legal advice on any questions about the law. Professional and regulatory organizations typically have frequently asked questions available, and advisors who can help as well. The right guidance can help to protect the professional and enable them to use data to benefit themselves and their clients.

ACKNOWLEDGMENTS

The authors thank Professors Emeka Oguejiofor and Brittany MacDonald-MacAulay (Department of Engineering, St. Francis Xavier University) for general guidance, and the *IIBEC Interface* peer reviewers, whose thoughtful advice and comments improved this paper immensely. Any errors remain those of the authors.

REFERENCES

1. Mason, R. 1986. "Four Ethical Issues of the Information Age" *MIS Quarterly* Vol. 10(1) pp. 5–12. https://www.jstor.org/stable/248873.
2. Maxwell, W. 2015. "Principles-Based Regulation of Personal Data: The Case of 'Fair Processing.'" International data privacy law 5.3: 205–216 at 206. doi:10.1093/idpl/ipv013.
3. Organization for Economic Cooperation and Development. 1980 and 2013. *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0188.
4. M. Dennedy, J. Fox, and T. Finneran. 2014. *The Privacy Engineer's Manifesto Getting from Policy to Code to QA to Value.* 1st ed. Berkeley, CA: Apress at p. 42.
5. Wilkinson, M., M. Dumontier, I. Aalbersberg, et al. 2016. "The FAIR Guiding Principles for Scientific Data Management and Stewardship" *Sci Data* 3, 160018, https://doi.org/10.1038/sdata.2016.18.

Please address reader comments to:
chamaker@iibec.org, including "Letter to Editor" in the subject line, or IIBEC, IIBEC Interface Journal, 434 Fayetteville St., Suite 2400, Raleigh, NC 27601.

ABOUT THE AUTHORS

Margaret H. McKay, MSc, JD

Margaret H. McKay, MSc, JD, leads the National Research Council of Canada's Artificial Intelligence for Logistics program, including its data ethics and responsible data activities. McKay holds degrees in biochemistry and law and is a certified Project Management Professional and a Certified Information and Privacy Professional (Canada).

Alana Gin, Dip. Eng.

Alana Gin, Dip. Eng. is a recent graduate of St. Francis Xavier University with a diploma in engineering. She has an interest in ethics and accountability in engineering practice, and she is continuing her studies in mechanical engineering at Dalhousie University.

special interest

PAY INCREASES ARE DRIVING THE GREAT RESIGNATION

In the past year, approximately 47 million American workers have changed jobs, and the reason is clear, wrote Julia Carpenter: Job-hoppers increase their pay by 6.4%, while those who stayed put saw their wages increase just 4.7%.

According to Yale professor Jennifer Dannals, employees used to change jobs because they were unhappy where they were working. Now they're motivated by higher pay.

But staying put can have its own advantages, especially when the economic outlook grows cloudy—or worse. During the 2008 recession, people who remained with their employers saw larger salary gains than those who job-hopped. And, Carpenter wrote, those who stayed didn't experience the anxiety of new-job unknowns, including the fear that those hired first might be terminated first during any downsizing at their new companies.

Source: *The Wall Street Journal*

SEDA ABACI/SHUTTERSTOCK.COM