# Privacy Data Management

Several issues ago, I wrote an article in this space titled, "Why Do We Need Data Privacy Laws?"[1] In that piece, I expressed my skepticism about many new privacy laws while the old ones were still not being observed. I would like to return to this subject, but from a very different perspective.

## Imperatives

I find that some proponents of data privacy consider it to be a moral imperative. In the European Union, it is formally stated to be a "fundamental right."[2] Others have framed privacy as an ethical issue.[3] Personally, I do not see privacy as either a right or a holy cause but rather as a principled way of doing business.

Of course, not everyone does the right thing just because it's the right thing. If there were no laws against theft, I would not steal my neighbor's lawnmower. Likewise, I do not need privacy laws to prevent me from spreading personal information about him. Ah, say the philosophers, I may be rejecting statutory laws, but instead I am falling back on *natural* law,[4] while Judeo-Christian clerics say the Ten Commandments govern all human behavior.[5] For myself, I need neither Aristotle nor Moses to tell me that I should not disclose personal information without the consent of the person involved.

## Attributes

Returning from that little philosophical tangent, let me say that as a businessperson who has had access to much information concerning other people over the course of my career, I respected their privacy and would have, with or without respect to any laws. Professionally, I have long advocated to keep all data secure, within the boundaries of their intended use. In addition, I have felt that information about people requires special handling, as defined in several frameworks, standards and, yes, laws.[6]

Thus, there is a category of data that can be distinguished from all others, based on certain of its attributes. Basic among these, of course, is a person's name.[7] Then there is any information which, when combined with a name, might definitively identify a specific individual. There are combinations of data items, *not* including a name, which would lead to identification of a specific person. For example, if you knew that there was someone who lives at 123 Main Street, works for ABC Company and attended State University in 2002, that person's identity could probably be determined. There are some databases, such as product catalogs, that do not contain personally identifiable information (PII) and, therefore, have no privacy interest, while others, such as customer records, are rife with PII.

> "IF THERE WERE NO PRIVACY LAWS, THE RULES FOR THE WAYS DATA MIGHT BE COLLECTED, USED, DISCLOSED AND DESTROYED COULD BE ENFORCED BASED ON THE ATTRIBUTES OF THE DATA THEMSELVES."

If there were no privacy laws, the rules for the ways data might be collected, used, disclosed and destroyed could be enforced based on *the attributes of the data themselves*. As I see it, this is the very definition of data management. (Well, in fairness, it is one definition of data management, which is a highly complex and much-debated field of knowledge.[8])

**Steven J. Ross,** CISA, CDPSE, AFBCI, MBCP
Is executive principal of Risk Masters International LLC. Ross has been writing one of the *Journal's* most popular columns since 1998. He can be reached at stross@riskmastersintl.com.

> TREATING PII AS DATA TO BE MANAGED RATHER THAN SEGREGATED WOULD, IN MY OPINION, LEAD TO GREATER CONSISTENCY IN ACCOMPLISHING PRIVACY.

## Ramifications

There are several ramifications to my characterization of data privacy as an aspect of data management. The first is that it positions data privacy legislation less as directives and more as a source for data rule sets. These rule sets are the definitions of characteristics that can be used to evaluate or validate specific conditions that are associated with a body of data.[9] Most privacy laws establish requirements for the use of PII and some do specify the attributes of PII. For example, the US Health Insurance Portability and Accountability Act (HIPAA) states 18 types of data elements that constitute healthcare-related PII, also called Protected Health Information (PHI).[10]

If the argument that data privacy as a subset of data management is a cogent one, then it follows that the privacy function in an organization should report to data management rather than the legal or compliance functions, where it is most likely to be found today.[11] This conclusion is, to say the least, controversial. One counterargument is that data management is a part of IT and, thus, cannot both make privacy policy and enforce it.[12] Structural concerns aside, treating PII as data to be managed rather than segregated would, in my opinion, lead to greater consistency in accomplishing privacy.

However, if the responsibility for privacy were to rest in the data management function, would privacy matters have sufficient visibility with senior management? The EU General Data Protection Regulation (GDPR) calls for the data protection officer to report to "the highest management level of the controller or the processor [of private information]."[13] Without joining the dispute as to whether a data protection officer is the same as a chief privacy officer,[14] it is legitimate to question whether the data manager is placed high enough to satisfy the GDPR's requirement. For that matter, is the chief legal or compliance officer sufficiently senior to meet it? A balance must be struck between effective control over privacy and the accountability of executive management.

## Conversation

The question as to whether privacy is an inherent attribute of personal data or is imposed by external laws may well be too theoretical for the people who actually have to do the job of securing data and ensuring that they are used in a fair and authorized manner. And, since the requirements are (or should be) the same, does it really matter? I believe it does, because if data privacy is to be achieved, managing data with structural rigor may achieve the goals of legislation without the need to scare the users into compliance based on the threats and penalties. I would far prefer to see privacy as an ethical way of doing business than as a burden that must be borne for statutory reasons. Moreover, I am not sure that scare tactics work anyway.

I hardly believe that this brief article is the last word on privacy and data management or, more specifically, about privacy being a characteristic of a certain class of data. There is some literature on privacy and data governance,[15] viewed from above, but none that I have seen addressing it from the bottom up based on the attributes of the data. I hope I do spur some conversation on the matter and would especially welcome hearing from colleagues who hold the Certified in the Governance of Enterprise IT® (CGEIT®) certification.

## Endnotes

1 Ross, S. J.; "Why Do We Need Data Privacy Laws?," *ISACA® Journal*, vol. 5, 2019, *www.isaca.org/archives*

2 European Commission, Charter of Fundamental Rights of the European Union (2012/C 326/02) EN 26.10.2012, *Official Journal of the European Union* C 326/391, Articles 7 and 8, 26 October 2012, *https://ec.europa.eu/info/aid-development-cooperation-fundamental-rights/your-rights-eu/eu-charter-fundamental-rights_en*

3 Lee, W. W., *et al*; "An Ethical Approach to Data Privacy Protection," *ISACA® Journal*, vol. 6, 2016, *www.isaca.org/archives*

4 Aristotle, *Nicomachean Ethics*, 5.7, translated by W. D. Ross (no relation), *http://classics.mit.edu/Aristotle/nicomachaen.5.v.html*, "Of political justice part is natural, part legal, natural, that which everywhere has the same force and does not exist by people's thinking this or that."

5 Of course, adherents of other religions do not recognize the Ten Commandments as law, though I do not find them to be more murderous, thieving or covetous than their Judeo-Christian counterparts.

6 Khan, M.; "A Guide to Selecting and Adopting a Privacy Framework," *ISACA Journal*, vol. 2, 2021, *www.isaca.org/archives*

7 In practice, this is far more complicated than it seems. Is Steven Ross the same person as Steven J. Ross (yes)? Steve Ross (yes)? Stephen Ross (no, but frequently misspelled anyway)?

8 The foundational document for data management is Data Management Association International (DAMA), *Data Management Body of Knowledge, 2nd Edition*, (DMBOK2), USA, 2017, *https://technicspub.com/dmbok/*. For a quick but still informative overview, I recommend our late ISACA® colleague, Ed Gelbstein's article, Gelbstein, E.; "Data Management Body of Knowledge—A Summary for Auditors," *ISACA Journal*, vol. 3, 2017, *www.isaca.org/archives*

9 InfoSphere Information Server, "Data Rule Definitions and Rule Set Definitions," IBM, USA, 2019, *https://www.ibm.com/docs/en/iis/11.7?topic=rules-data-rule-definitions-rule-set-definitions*. Note that this definition is related to a specific IBM product. Other vendors of data management tools have other definitions that I find to be largely the same.

10 Loyola University Chicago 150, "18 HIPAA Identifiers," Illinois, USA, 2021, *https://www.luc.edu/its/aboutits/itspoliciesguidelines/hipaainformation/18hipaaidentifiers/*

11 This statement is based on my personal experience and is supported by International Association of Privacy Professionals (IAPP), *IAPP-EY Annual Privacy Governance Report*, USA, 2019, p. 14, *https://iapp.org/resources/article/iapp-ey-annual-governance-report-2019/*. However, the IAPP's survey shows that privacy leaders reporting to legal counsel is prevalent in the United States, while in the European Union, they report most often directly to the board of directors.

12 Gerbs, Jack; private communication to the author. This counterargument in turn raises the question of whether data management should be in the IT organization at all.

13 Intersoft Consulting, Art. 38.3, GDPR Position of the Data Protection Officer, Belgium, 2016, *https://gdpr-info.eu/art-38-gdpr/*

14 Ashbel, A.; "Data Protection Officer vs. Chief Privacy Officer: A Comparison of Two Compliance-Related Roles," NetApp blog, 14 June 2020, *https://cloud.netapp.com/blog/cvo-blg-data-protection-officer-vs-chief-privacy-officer*

15 Salido, J.; P. Voon; *A Guide to Data Governance for Privacy, Confidentiality, and Compliance Part 1: The Case for Data Governance*, Microsoft Corporation, USA, January 2010, *http://mscorp.indsyntest.com/perspective/pdf/sec-Data_Governance_-_Moving_to_Cloud_Computing.pdf*

## Enjoying this article?

- Read *Ensuring Privacy Through Effective Data Management. www.isaca.org/ensuring-privacy-data-management*
- Learn more about, discuss and collaborate on information and cybersecurity in ISACA's Online Forums. *https://engage.isaca.org/onlineforums*