Identity Analytics And Belief Structures

Harry Katzan, Jr., Savannah State University, USA

ABSTRACT

Personal identity is an important topic in information systems in general and data analytics in particular. Normally associated with digital security and privacy, the scope of identity is much greater and affects most aspects of everyday life. Related subjects are behavioral tracking, personal-identifiable information (PII), privacy data relevance, data repurposing, identity theft, and homeland security. The purpose of this paper is to establish a context for using analytics to combine evidence to categorize certain subjects based on belief structures.

Keywords: Identity, privacy, evidence, belief

INTRODUCTION

Identity is a major issue in the security of modern information systems and the privacy of data stored in those systems. Security and privacy concerns are commonly associated with behavioral tracking, personal-identifiable information (PII), the relevance of private data, data repurposing, identity theft, and homeland security. We are going to approach the subject from a data analytic viewpoint, where the primary challenge is to use identity in an effective way to determine group membership. Instead of focusing on the protection of identity in this paper, we are going to propose methods for using identity to make essential judgmental decisions.

Identity

Identity is a means of denoting an entity in a particular namespace and is the basis of security and privacy – regardless if the context is digital identification or non-digital identification. We are going to refer to an identity object as a *subject*. A subject may have several identities and belong to more than one namespace. A pure identity denotation is independent of a specific context, and a federated identity reflects a process that is shared between identity management systems. When one identity management system accepts the certification of another, a phenomenon known as "trust" is established. The execution of trust is often facilitated by a third party that is acknowledged by both parties and serves as the basis of digital identity in computer-based information systems and personal recognition is social affairs. (Salido 2010) There is another side to personal recognition. We are often afforded the identity of a person based on the judgment of a third party and are obligated to respond to that assessment. It would seem to be prudent in a civilized society to obtain additional information on the subject and combine the various items of information to obtain a composite view before engendering a timely response to the situation.

Privacy

Information systems typically process and store information about which privacy is of paramount concern. The main issue is identity, which serves as the basis of privacy or lack of it, and undermines the trust of individuals and organizations in other information-handling entities. The key consideration may turn out to be the integrity that organizations display when handling personal information and how accountable they are about their information practices. From an organizational perspective, control over information should remain with the end user or the data's creator with adequate controls over repurposing. From a personal perspective, a person should have the wherewithal to control his or her identity as well as the release of socially sensitive identity attributes. (Cavoukian 2009, 2010, ACLU 2010, CDD 2009, OECD 2010, FBI 2004) One of the beneficial aspects of the present concern over information privacy is that it places the person about whom data are recorded in proper perspective. Whereas

such a person may be the object in an information system, he or she is regarded as the subject in privacy protection – as mentioned earlier. This usage of the word *subject* is intended to imply that a person should, in fact, have some control over the storage of personal information.

More specifically, the *subject* is the person, natural or legal, about whom data is stored. The *beneficial user* is the organization or individual for whom processing is performed, and the *agency* is the computing system in which the processing is performed and information is stored. In many cases, the beneficial user and the subject are members of the same organization.

The heart of the issue is privacy protection, which normally refers to the protection of rights of individuals. While the concept may also apply to groups of individuals, the individual aspect of the issue is that which raises questions of privacy and liberty. On the other hand, as in the case of terrorism and homeland security, privacy runs contrary to societal needs. We are going to keep those considerations in mind in this paper.

Belief

Belief is often regarded as a mental state in which a person holds a proposition to be true without necessarily being able to prove its truth to other persons. Even though absolute certainty is not required with belief, a person's set of beliefs can play an important role in the causation of behavior. Belief is associated with rational behavior and behavior that is not totally rational. Belief has a lot to do with a believer's mind. If a representation for belief P exists in a person's mind, then it is an *explicit belief.* If a representation for belief Q does not exist in a person's mind but is based on another proposition P, then it is an *implicit* belief. Beliefs that are based on an associative relationship are usually regarded as implicit beliefs.

Some authors classify beliefs as being epistemic versus pragmatic and dispositional versus occurent. (Stanford 2010) With an *epistemic belief*, there is evidence for the belief. With *pragmatic belief*, there are practical reasons for the belief. Having been engaged in terrorist training, for example, would probably yield an epistemic belief that the subject has some inclination for terrorism. Pascal's argument to believe in God is an example of a pragmatic belief. It reads as follows: "The consequences of failing to believe in Him if he exists (eternal fire and damnation) are much worse than the consequences of believing in Him if he does not exist (sin avoidance and contrition)."

Dispositional belief refers to the supposition that the subject is disposed to possess a certain stance on a topic or is inclined to a particular behavior. *Occurent belief* refers to the assumption that the subject is actually performing a sequence of actions. The penultimate example is also an example of dispositional belief. Direct knowledge, or information obtained from a trusted source, that a subject is performing a certain action is associated with occurent belief. In the latter case, verification of identity may be of some concern and be the difference between "belief in" and "knowledge of."

IDENTITY THEORY

The notion of identity is an important subject in philosophy, mathematics, and computer information systems. In its most general sense, identity refers to the set of characteristics that makes a subject definable. Each characteristic can be viewed as a single point in a three-dimensional Cartesian coordinate system where the axis are *subject, attribute,* and *value*. (Katzan 1975) Thus, the fact that George is twenty-five years old could be denoted by the triple <George, age, 25>. A set of characteristics over a given domain can uniquely identify a subject. This simple concept is the basis of identity and privacy in business, government operations, and everyday life. The notion of identity applies to organizational subjects as well as to personal subjects. An important aspect of modern identity theory is the linking of identity namespaces.

Knowledge and Power

The phrase "knowledge is power" is a popular means of expressing the value of information. So popular, in fact, that one would think its origin is the modern age of computers and information technology. That

assumption, however, is not correct. The first reference that could be found is credited to the famous Sir Francis Bacon is his book, published in 1605, entitled *Advancement of Learning*, quoted as follows: (Bacon 1605)
But yet the commandment of knowledge is yet higher than the commandment over the will: for it is a commandment over the reason, belief, and understanding of man, which is the highest part of the mind, and giveth law to the will itself. For there is no power on earth which setteth up a throne or chair of estate in the spirits and souls of men, and in their cogitations, imaginations, opinions, and beliefs, but knowledge and learning.

Knowledge, in the sense that it is information concerning a thing or a person, can be used to further one's endeavors or it can be used to control a subject, thus diminishing its freedom and liberty. The protection of personal privacy is a Fourth Amendment right, and identity is the basis of privacy. The following sections give a philosophical view of identity.

Knowledge, Attributes, and Identity

Identity is primarily used to establish a relationship between an attribute or set of attributes and a person, object, event, concept, or theory. The relationship can be direct, based on physical evidence, and in other cases, the relationship is indirect and based on a reference to other entities. In a similar vein, the relationship can be certain or uncertain, and in the latter case, based on deduction or inference. The relationship determines an element of knowledge. For example, the knowledge element "you are in your car" is a statement in which "you" and "your car" are things that exist and the "in" is a relationship. Direct knowledge is known by *acquaintance* and is evidenced by a physical connection. Indirect knowledge is determined through a reference to a particular with which the analyst is acquainted. This form is known as knowledge by *description*. (Russell 1912) *Direct knowledge* is determined through sense data, memory, or introspection. *Indirect knowledge* is determined through a reference to another particular, as in "the person who ran for congress in 2004" or through a form of self-awareness where what goes on in subject's mind, for example, is estimated by an analyst's interpretation based on experience or self-evaluation.

Synthetic knowledge reflects certainty based on evidence inherent in the attribute values at hand. *Analytic knowledge* reflects a degree of uncertainty and is determined by deduction, as in "he is the only person with that 'attribute value'," or by inference based on known particulars, such as "all terrorists have beards." Inference, in this case, could be regarded as a form of derivative knowledge. The value of analytic knowledge is that it enables the analyst to exceed his or her limit of private experience. (Kant 1787) The concepts of knowledge, attributes, and identity are summarized in Table 1.

Table 1. Elements of knowledge and identity

	Synthetic	**Analytic**
By acquaintance	A particular of which we have direct knowledge.	A particular of which we have knowledge based on deduction.
By description	A particular of which we have indirect knowledge by reference to a particular with which we are acquainted.	A particular of which we have indirect knowledge through inference (derivative knowledge).

Numerical and Qualitative Identity

Identity refers to the characteristics that make a subject the same or different. We are going to establish two forms of identity: numerical and qualitative. Two subjects are *numerically identical* if they are the same entity, such that there is only one instance. Two subjects (or objects in this case) are *qualitatively identical* if they are copies or duplicates. In the popular movie *The Bourne Identity*, for example, the characters *Jason Bourne* and *David Web* are numerically identical, and the number of subjects is one. So it is with *Superman* and *Clark Kent* in another domain. On the other hand, a set of animals with the same biological characteristics – e.g., a species – is regarded as being qualitatively identical. The notion of qualitative identity is remarkably similar to the modern definition of a *category* informally defined as a collection of entities with the same characteristics, having the same values for the same attributes.

Theory of the Indiscernibles

An important aspect of identity theory is that subjects exhibit features of permanence and change, analogous to sameness and difference mentioned previously. We are going to discuss the concept of temporal identity in the next section. The notion of change implies a subject that undergoes a transformation and also possesses a property that remains unchanged. Both Locke and Hume[1] have proclaimed that change reflects the idea of unity and not of identity. Leibnitz proposed the *Theory of Indiscernibles* suggesting that subjects (i.e., objects or entities) that are indiscernible are identical. (Stroll 1967) The subject of indiscernibles has implications for cloud computing, information systems, and change. To what extent a change in a characteristic denotes a change in identity is an open item at this time and implies that there is a probabilistic aspect to identity.

Russell approaches the subject of identity from an alternate viewpoint, analogous to definite and indefinite articles. Russell proposes that a description may be of two sorts: definite and indefinite. A definite description is a name, and an indefinite description is a collection of objects x that have the property Ø, such that the proposition Øx is true. (Russell 1919) In the phrase *Dan Brown is a famous author*, for example, 'Dan Brown" is a name and the indefinite description is obvious, leading to the probabilistic link between a subject and a characteristic.

Temporal Identity

There is a rich quantity of philosophical literature on the change of identity over time. Are you the same person you were yesterday? Are there persistent attributes that allow for positive identity between time periods? As mentioned previously, entities in everyday life exhibit features of permanence and change. In the domain of personal identity, address attribute is a primary candidate for change. For example, John Smith lives at 123 Main Street. He moves out and another John Smith moves in. This is distinct possibility in a crowded city.

There is a form of *attribute duality* between a person subject and an object subject. A subject – an object, such as a residence, in this case – is characterized by who lives there. For example, rich people live on Sutton Place in New York. The discussion leads to four related concepts: endurant identity, perdurant identity, endurant attribute, and perdurant attribute. Clearly, the term *endurant* refers to a noun that does not change, where perdurant refers to one that does. Thus, the identity problem is essentially translated to an operant problem of "recognizing identity."

BELIEF STRUCTURES

We are going to assign subjects to an identity set based on values of attributes that characterize that set. An *identity set* is analogous to a namespace except that we are going to view identity from an analytic basis rather than from a privacy and security perspective. Consider the following scenario:

We are trying to identify subjects that belong to a certain group G. We know about the group G and its attributes. We have a paid knowledge source K_1 that informs us that subject A is a member of G. However, K_1 is not always correct, and we know that. We have used K_1 enough to know that he provides us with information when he needs money. We have an intuitive belief of how often he is correct. Fortunately, we have another source K_2 that can supply similar information. K_2 is not as hungry for money as K_1, and his opinion frequently runs contrary to K_1's. We would like to use analytics to combine the information from K_1 and K_2 so as to obtain a composite picture of the situation. Our resultant belief of A's membership in G is not the end of the story. The belief that we obtain of A's membership in G could then be propagated down the line to other analytic situations. However, we are going to go beyond the notion that even though subject A possesses G's attributes, it doesn't necessarily indicate that A is a member of identity set G.[2]

[1] Locke (*An Essay concerning Human Understanding*, Book II, Chapter 27) and Hume (*A Treatise of Human Nature*, Book I, Part IV).

[2] Consider the following statements. *All spies wear blue trousers. George wears blue trousers. Therefore, George is a spy.* The analysis does not hold unless we have corroborative evidence.

We are going to use belief structures, compatibility relations, consensus theory, and belief propagation to attack this problem. Consensus theory is a methodology for combining evidence based on Dempster-Shafer theory (Shafer 1976; Katzan 1992, 2006) and the mathematical combination of evidence (Dempster 1967). Consensus theory has commanded a considerable amount of attention in the scientific and business communities, because it allows a knowledge source to assign a numerical measure to a proposition from a problem space and provides a means for the measures accorded to independent knowledge sources to be combined. Consensus theory is attractive because conflicting, as well as confirmatory, evidence from multiple sources may be combined.

Frame of Discernment

A frame of discernment is a means of representing the possibilities under consideration, as in the following example:

V = {medicine, law, education}

Clearly, the elements in a frame of discernment are, in fact, propositions that can be interpreted as events or states. Thus, if component s_i of system S over domain V were associated with the symbol **law,** then that state is equivalent to the proposition, "The true value of V for component s_i is **law**," or in ordinary language, "s_i prefers **law**." Accordingly, the set S of propositions S_i, S = $\{S_1,S_2,\ldots,S_n\}$ represents the collection of states of a system under analysis. Clearly, at an agreed upon point in time, one proposition is true and the others are false.

The basis of identity analytics is a frame of discernment (Θ). Accordingly, a knowledge source may assign a numerical measure to a distinct element of Θ, which is equivalent to assigning a measure of belief to the corresponding proposition. In most cases, the numerical measure will be a belief assignment. A measure of belief may also be assigned to a subset of Θ or to Θ itself. Consider a frame of discernment Θ and its power set denoted by 2^{Θ}. Given the frame Θ = {a, b, c}, its power set is delineated as: 2^{Θ} = {{a, b, c}, {a, b}, {a, c}, {b, c}, {a}, {b}, {c}, {ϕ}}. In identity analytics, a knowledge source apportions a unit of belief to an element of 2^{Θ}. This belief can be regarded as a mass committed to a proposition and represents a judgment as to the strength of the evidence supporting that proposition. When viewed in this manner, evidence focuses on the set corresponding to a proposition; this set is called a *focal set*. The support for a focal set is a function m that maps an element of 2^{Θ}, denoted by A, onto the interval [0,1]. Given a frame of discernment Θ and function m: $2^{\Theta} \rightarrow$ [0,1], a support function is defined as: $m(\phi) = 0$, where ϕ is the null set, $0 \le m(A) \le 1$, and $\sum_{A \subset 2^{\Theta}} m(A) = 1$.

A simple support function assigns a measure of belief to the focal set A, as: $m(A)>0$; $m(\Theta)=1-m(A)$; and $m(B)=0$, for all $B \subset 2^{\Theta}$ and $B \neq A$. The simple support function for a focal set A assigns a portion of the total belief exactly to A and not to its subsets or supersets. The remainder of the belief is assigned to Θ, because certainty function must add up to 1, $m(\Theta) = 1-m(A)$. It is possible that a body of knowledge or evidence supports more than one proposition, as in the following case. If Θ = {a, b, c, d}, A = {a, b}, and B = {a, c, d}, then the evidence supports two focal sets, which in the example, are A and B. If $m(A) = 0.5$ and $m(B) = 0.3$, then $m(\Theta) = 0.2$. A support function with more than one focal set is called a *separable support function*. Separable support functions are normally generated when simple support functions are combined. The notion of combining simple support functions is a practical approach to the assessment of evidence. An analyst obtains information from a knowledge source, and it leads to an immediate conclusion – not with certainty, but with a certain level of belief. This is a straightforward means of handling human affairs and is precisely what people do when analyzing situations in everyday life. If additional information comes in, the various pieces of evidence are combined to obtain a composite picture of the situation.

Compatibility Relations

In this particular instance, we are going to establish relations between three sets and the frames of discernment for K_1, K_2, and A, where the K_i are the knowledge sources and A is the subject. The relations will be

represented as:

$K_1 \rightarrow$ A
$K_2 \rightarrow$ A

and the frames:

A = {m, n}
K_1 = {r, u}
K_2 = {c, i}

The question is whether A is a member of G, denoted by m, or not a member of G, denoted by n. As far as K_1 is concerned, he might be telling us what he thinks we want to hear, so his judgment is classed as reliable, denoted by r, or unreliable, denoted by u. K_2 is simply correct or incorrect, denoted by c or i, respectively.

We can now establish the requisite compatibility relations, based on the fact that K_1 informs us that A is a member of G, and K_2 informs us that A is not a member of G.

1. If K_1 has based his opinion on credible evidence and is operating in a trustworthy manner, then he is in state r that is compatible with state m for A. If K_1 just needs the money or doesn't have good evidence, then he is in state u that is compatible with both states m and n. Thus, we have the compatibility relation:

{(r, m), (u, m), (u, n)}

2. If K_2 is behaving as normal, and there is no reason at this point not to accept that, then he is in state c that is compatible with state n for A. If K_2 is in state i then all bets are off, and this state is compatible with A's states m and n. We then have the second compatibility relation, which is:

{(c, n), (i, m), (i, n)}

Compatibility relations will allow us to assign belief to the assertions of K_1 and K_2 and propagate that belief through the belief network, resulting in a set of focal sets that can be combined using Dempster's rule in order to obtain a composite picture of the situation. Up to this point, we are working in the problem space for the analysis.

Prior Belief

An analyst assigns a measure of credibility to a knowledge source. In our example, let the belief assigned to K_1 be denoted by p and the belief assigned to K_2 be denoted by q, yielding the following prior belief:

Source	*Belief*
K_1	{[(r), p]. [(r, u), 1-p]}
K_2	{[(c), q]. [(c, i), 1-q]}

Since we are in the problem space, our belief in K_1 and K_2 is invariant.

Belief Propagation

Belief propagation transfers the knowledge from the problem space to the solution space using the compatibility relations, resulting in the following focal sets:

Source	*Focal Set*
K_1	{[(m), p]. [(m, n), 1-p]}

K_2 {[(n), q]. [(m, n), 1-q]}

The results of belief propagation assign the mass of the information received from K_1 to (m) and the remainder of the belief is assigned to (m, n), which is the frame, denoted by Θ in the above introduction. A similar argument applies to K_2 such that the mass of that belief is assigned to (n) and Θ, respectively.

Combination of Evidence

Using Dempster's rules of combination (Dempster op cit.), the resulting focal sets can be combined yielding the following assessment in the solution space:

$$\left[(m), \frac{p(1-q)}{1-pq}\right], \left[(n), \frac{(1-p)q}{1-pq}\right]. \left[(m,n), \frac{(1-p)(1-q)}{1-pq}\right]$$

using symbolic math from calculations in *Mathematica*™. Applying the expression to several values of p and q yields the following results:

K_1 (p)	K_2 (q)	$K_1 \oplus K_2$
.6	.7	{[(m), 0.310], [(n), 0.483], [(m, n), 0.207]}
.7	.8	{[(m), 0.318], [(n), 0.545], [(m, n), 0.136]}
.8	.9	{[(m), 0.286], [(n), 0.643], [(m, n), 0.071]}
.7	.5	{[(m), 0.538], [(n), 0.231], [(m, n), 0.231]}

This is what we wanted to show. QED.

SUMMARY

We have introduced the theory of identity and applied it to the combination of knowledge for assessment of whether a subject is a member of a certain group. We have introduced belief structures and a relevant methodology for mapping a problem space into a solution space.

APPENDIX: COMBINATION OF EVIDENCE

A method of combining evidence is known as Dempster's rule of combination (Dempster 1967). Evidence would normally be combined when it is obtained from two different observations, each over the same frame of discernment. The combination rule computes a new support function reflecting the consensus of the combined evidence.

If m_1 and m_2 denote two support functions, then their combination is denoted by $m_1 \oplus m_2$ and is called their *orthogonal sum*. The combination $m_1 \oplus m_2$ is computed from m_1 and m_2 by considering all products of the form $m_1(X) \bullet m_2(Y)$, where X and Y range over the elements of Θ; $m_1(X) \bullet m_2(Y)$ is the set intersection of X and Y combined with the product of the corresponding probabilities.

For example, consider the frame of discernment

Θ = {h, t, s}

and views A and B, based on two different observations over the same frame:

X = {{h},0.6},{{t},0.3},{{s},0.1}}
Y = {{h},0.4},{{t},0.4},{{s},0.2}}

The entries are combined, as follows, using Dempster's rule of combination:

$m_1 \oplus m_2(\{h\}) = 0.24$
$m_1 \oplus m_2(\{t\}) = 0.12$
$m_1 \oplus m_2(\{s\}) = 0.02$
$m_1 \oplus m_2(\{Ø\}) = 0.62$

Thus, for $A_i \cap B_j = \boldsymbol{A}$ and $m_1 \oplus m_2 = \boldsymbol{m}$, the combination rule is defined mathematically as:

$$\boldsymbol{m}(\boldsymbol{A}) = \sum_{A_i \cap B_j = \boldsymbol{A}} m_1(A_i) \bullet m_2(B_j) / \left(1 - \sum_{A_i \cap B_j = Ø} m_1(A_i) \bullet m_2(B_j)\right)$$

The denominator reflects a normalization process to insure that the pooled values sum to 1. So, in this instance, the normalization process yields the combination

X⊕Y = {{h},0.63},{{t},0.32},{{s},0.05}}

after normalization by dividing the combined assessment by (1-0.62) or 0.38. Because the problem is well-structured, the representation can be simplified as

X⊕Y = {0.63,0.32,0.05}

For views A = $\{A_1, A_2, \ldots, A_n\}$ and B=$\{B_1, B_2, \ldots, B_n\}$, the combination rule can be simplified as

$$A \oplus B = \{A_1 \times B_1/k, A_2 \times B_2/k, \ldots, A_n \times B_n/k\}$$

where

$$k = \sum_{i=1}^{n} A_i \times B_i$$

We will refer to latter the equation as the *simplification rule*. (Katzan 2009) Readers are directed to Shafer (1976) and Katzan (1992) for additional information on Dempster's rule of combination.

ACKNOWLEDGMENT

Thanks for Margaret Katzan for reading the manuscript.

AUTHOR INFORMATION

Dr. Harry Katzan teaches at Savannah State University and is the founding editor of the *Journal of Service Science*.

REFERENCES

1. Bacon, Sir Francis. 1605. *Advancement of Learning*. (Republished in the *Great Books of the Western World*. Volume 30, Robert Maynard Hutchins, Editor in Chief, Chicago: Encyclopedia Britannica, Inc., 1952).
2. Black, M. 1952. Identity of Indiscernibles. *Mind* 61:153. (Secondary reference.)
3. ACLU of Northern California. 2010. *Cloud Computing: Storm Warning for Privacy?* www.dotrights.org, (downloaded 3/11/2010).
4. Cavoukian, A. 2009. *Privacy in the Clouds*. Toronto: Information and Privacy Commission of Ontario (www.ipc.on.ca).

5. Cavoukian, A. 2010. 7 Laws of Identity: The Case for Privacy-Embedded Laws of Identity In the Digital Age." Toronto: Information and Privacy Commission of Ontario (www.ipc.on.ca).
6. Center for Digital Democracy (CDD). 2009. Online Behavioral Tracking and Targeting: Legislative Primer September 2009. www.democraticmedia.org/privacy-legislative-primer. (downloaded 3/11/2010).
7. Dempster, A.P. 1967, "Upper and Lower Probabilities Induced by a Multivalued Mapping," *The Annals of Statistics* 28:325-339.
8. Federal Bureau of Investigation. 2004. Privacy Impact Assessment. www.fbi.gov/biometrics.htm. (downloaded 2/20/2010).
9. Kant, I. 1787. *Critique of Pure Reason*. (Republished in *Basic Writings of Kant*. Allen W. Wood, Editor, New York: The Modern Library, 2001).
10. Katzan, H. 1975. *Computer Data Management and Data Base Technology*, New York: Van Nostrand Reinhold Co.
11. Katzan, H. 1992. *Managing Uncertainty: A Pragmatic Approach*, New York: Van Nostrand Reinhold Co.
12. Katzan, H. 2008. Categorical Analytics Based on Consensus Theory. *Journal of Business and Economics Research*, 6(8), 89-102.
13. Katzan, H. 2010. On the Privacy of Cloud Computing. *International Journal of Management and Information Systems*, (accepted for publication).
14. OECD 2010. OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. www.oecd.org. (downloaded 3/23/2010).
15. Russell, B. 1912. *The Problems of Philosophy*. (Republished by Barnes & Noble, New York, 2004).
16. Russell, B. 1919. *Introduction to Mathematical Philosophy*. (Republished by Barnes & Noble, New York, 2005).
17. Salido, J. and P. Voon. 2010. A Guide to Data Governance for Privacy, Confidentiality, and Compliance: Part 1. The Case for Data Governance. Microsoft Corporation.
18. Shafer, G. 1976, *A Mathematical Theory of Evidence*, Princeton, NJ: Princeton University Press.
19. Stroll, A. 1967. *Identity*. (Entry in *The Encyclopedia of Philosophy*, Volume 4, Paul Edwards, Editor-in-Chief, New York: Macmillan Publishing Co., 1967).

NOTES