Questioning Trust in the Era of Big (and Small) Data
by Kristene Unsworth

The issues covered by information policies are far-reaching and in many cases touch on our individual relationships with government agencies and corporate entities. In the June/July 2014 edition of the Bulletin 1 consolidated a number of accepted definitions of information policy and called for the need to articulate the importance of data as the fundamental part of information [1]. This view follows the standard understanding of the progression from data to information and finally knowledge.

It is no longer the fact that we are in control of our personal information, let alone the many data points that we leave throughout our daily activities. Of course, some organizations like Target, Amazon or Google (to name only a few) provide users with documentation that lays out what the business will or will not do with the information they collect when any of us visit their pages or in some cases walk in their doors. Such terms of service, privacy policies and statements related to third-party sharing are all attempts made by organizations to cover the legal terrain by posting policies for users to read and acknowledge their agreement.

The fact that few users actually read these documents is not the point. From a legal standpoint the documents exist and users have implicitly through use of the site or explicitly through indicating agreement to the policy read the content and agreed to what is laid forth. Our signature or mark on the form binds us to these agreements. Yet this is old news. We know that companies follow our shopping patterns and trace our actions online. Trust may be a value that we hold in our relationships with others, but it is also held alongside other values. In some cases it may be safe to say we trust that our personal information will be used in a variety of ways in spite of established privacy policies and guidelines.

Information policy conversations about privacy, security, personally...
identifiable information, net neutrality and global information flows come back to the need for more than laws, rules and regulations. Whether we can trust others with our information is at the crux of the debates. An oft-cited piece by Helen Nissenbaum, *Securing Trust Online: Wisdom or Oxymoron*, begins with the statement, “the way we stipulate the conditions of the online world may be decisive for whether or not trust is achieved.” [2, p. 635] Though written over a decade ago the statement is still timely. From eHealth to the privacy considerations of digital readers, information policy/trust issues hold a prominent place in social and political arenas. In many cases technologies are used, and the rules and regulations governing them are pushed aside to be dealt with when and if a problem arises. Often we are playing a game of catch up crafting legislation related to information technology.

In many cases, privacy is the main concern voiced in relation to policies that govern the collection, retention and use of information, but, ultimately, these issues come down to whether we can trust the government agency or corporate entity with our personal information. Bruce Schneier quotes the philosopher Sissela Bok in his book *Liars and Outliers*: “Whatever matters to human beings, trust is the atmosphere in which it thrives.” [3, p. 7] Trust is also part of the bedrock of society and a necessary element in the contract between individuals and the government. Members of the Special Interest Groups/Information Policy (SIG/IFP) and International Information Issues (SIG/III) are eager to address these types of relationships between trust, society and information. To this end, the first SIG/IFP-SIG/III annual workshop in information policy issues, “Trust in the Age of Data (Big and Small),” will be held on October 31, 2014, at the ASIS&T Annual Meeting in Seattle, Washington. Our goal is to provide a space for inquiry into the elements of trust in light of ongoing data collection and use throughout society (both commercial and governmental).

We plan [4] to address questions such as

- What are the economic, political and legal implications of trust in the age of data (big and small)?
- How does policy design build/undermine trust?
- What are the ethics of trust in the age of data?
- How are researchers conceptualizing trust in the age of data?
- How can scholars investigate infrastructures of trust?
- Are understandings of trust shifting? If so, with what consequences, in which contexts?
- When is trust justified? When is it not justified? Should decision-makers focus on and build trustworthiness rather than (mere) trust?
- What are the economic, political and legal implications of trust in the age of data (big and small)?
- How does policy design build/undermine trust?
- What are the ethics of trust in the age of data?
- How are researchers conceptualizing trust in the age of data?
- How can scholars investigate infrastructures of trust?
- Are understandings of trust shifting? If so, with what consequences, in which contexts?
- When is trust justified? When is it not justified? Should decision-makers focus on and build trustworthiness rather than (mere) trust?

Discussions of information policy are often based in the larger context of governing or the infrastructure in which social and political norms are established. The U.S. Constitution, the Constitution of Canada, the United Nations Declaration of Human Rights and other guiding documents exemplify these foundations. Democracy and fairness are based in transparency and access to information. The “right to information” is nonnegotiable and conceptualized most frequently as our right to access information about the goings on of our government. There is also the commonly held assumption that the information we get is true. In order for democracy to flourish, we must trust our government. Sandra Braman’s excellent book, *Change of State: Information, Policy and Power*, makes the strong connection between information policy and democratic ideals [5]. She focuses on some of the areas in the U.S. Constitution that insure the right of citizens to information about their government. The right to information is not only about access, but also about privacy.

The Fourth Amendment of the U.S. Constitution has been interpreted as calling for a right to privacy:

The right of the people to be secure in their persons, houses, papers and effects against unreasonable searches and seizures, shall not be violated, and no warrants shall issue but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched and the persons or things to be seized [6].

Without some degree of trust in the written word of the Constitution and the authorities that carry it out the agreement made between each of us and the societies to which we belong, trust breaks down. Some have questioned whether the massive data gathering and use we experience today has already changed this social contract. It is not the collection of these data traces that is troublesome but the potential that the data may be used in ways that erode our sense of trust in organizations and government.

For some, trusting the government is already a mistake, “…trusting the
government with your privacy is like trusting a Peeping Tom with your window blinds.” [7] Whether we approach the issue of trust in relation to privacy, we do know that our daily activities leave a digital trace. We can only trust that organizations and the government will use these bits in a way that comports with our conceptions of trust. Transparency is crucial in this case because, if we don’t know what or how data is being used, we can only rely on the words and actions of organizations and governmental agencies.

The question of trust is not limited to how we can best ensure it via policy, but is important across all ASIS&T special interest groups. Whether we trust in the authenticity of digital collections or in the validity of retrieval results, trust is a cornerstone of this professional organization. We hope to attract a broad spectrum of ASIS&T members as well as practitioners and individuals who may not yet belong to ASIS&T in our attempt to better understand and conceptualize trust in the age of data.

Resources Mentioned in the Article


[4] These questions are taken from the SIG/IPF-SIG/III workshop description to be published in the ASIS&T Annual Meeting Proceedings.

