THE Information Accountability Foundation
COLLABORATIVE POLICY INNOVATION

From IAPP blog, 6 September, 2013

Accountability Is About Values

By Martin Abrams

September 06, 2013

Accountability

Over the past year, I reflected on why I have been doing privacy for nearly a quarter of a century. As privacy professionals, you and I do privacy because we believe people shouldn't be afraid of being harmed by the digitization of their pathways through life. We do privacy so young adults may evolve into the people they will be, rather than be predestined by mathematics. We do privacy so individuals may think new thoughts, explore new concepts and converse with others without painting a black-and-white picture of themselves rather than one that reflects a thousand shades of grey or a rainbow of color. We do privacy because we believe privacy is fundamental to human dignity and freedom. After reflection, I decided it is time for me to focus on the role of values in privacy. So today I begin a new journey leading the Information Accountability Foundation.

Institutionalizing accountability requires focused work in all segments of the privacy community: private sector, enforcement agencies, policymakers and civil society. Late last year, a number of companies from the global accountability project founded the Information Accountability Foundation (IAF) to focus on institutionalizing accountability in business practices, regulatory oversight and the next generation of privacy law. The IAF is incorporated as a nonprofit charitable organization so that enforcement agencies and civil society may be integral in all its processes. The IAF was created to facilitate that focus. By doing so, it will assure that the key values of data use creating benefit, not causing harm, and being respectful of dignity are all in place. In taking a leadership role at the IAF, I am returning to my roots and focusing my attention on integrating values into privacy implementation, enforcement and legislation.

"Institutionalizing accountability requires focused work in all segments of the privacy community: private sector, enforcement agencies, policymakers and civil society."

Martin Abrams

Values have always been the foundation for privacy management. Twenty years ago, I cornered my boss's boss, the group CEO, at breakfast while we were traveling. The company, TRW Information Systems and Services, had gone through a rough privacy patch after inaccurately reflecting tax bills as liens on many of the credit reports in Vermont. As director of consumer policy, I was searching for a way to connect privacy to everyone's job as part of creating a new privacy culture. I told the CEO that we had to discover our information values, embrace them and use them in making information management decisions based on those values, not just the law.

With his blessing I put together a team of middle-level managers. Within a few weeks, we agreed on core information values and began socializing those values both up and down the organization. Those values include:

- **Balance,** which requires the organization take into consideration both the economic and privacy interests of individuals;
- **Accuracy,** which speaks to data being up to the task and individuals' ability to participate in the process;
- **Security,** which reinforces that there is no privacy if data is not secure;
- **Integrity**, which requires compliance with both the law and the expectations for appropriate information use;
- **Communication,** which obligates the organization to inform the public of data use and choices and educate all stakeholders about data.

While these values contain many of the elements of Fair Information Practice Principles, they go beyond those principles to make data stewardship an ethical issue for the company. They also acknowledge that information usage is about creating benefits, not just for the organization but also the individual to whom the information pertains. In 1992 we were in the early days of making the transition from an industrial era where information facilitated the improvement of business processes, to an information age where information would be the defining element in economic growth. It was

clear to me that information policy was not about standing in the way of benefit creation but rather freeing data users by providing the means for civilly governing data applications.

Fast-forward 20 years, and we find that values are really the key to accountability, which I believe is the future of privacy. Accountability is where organizations take ownership for the management of the information they collect and use and understand and mitigate the risks they create for individuals. Furthermore, accountable organizations stand ready to demonstrate their data stewardship to privacy enforcement agencies. Accountability is the mechanism for organizations to become Big Data practitioners, using data to be innovative while still protecting individuals. Accountability is required by many data protection systems and suggested by many more.

> *"Values are really the key to accountability, which I believe is the future of privacy."*
>
> **Martin Abrams**

Over the past five years, privacy leaders from government, enforcement agencies, civil society and business, with the Centre for Information Privacy Leadership as secretariat, have done a great job of creating the opportunity for accountability to be operationalized by giving flesh to the accountability principle. However, to fully integrate accountability into privacy processes requires focus and participation, including funding, from all stakeholders. A nonprofit was necessary to achieve this initiative.

In late April, I decided that it was time to retire from the Centre for Information Policy Leadership. Because of my passion for accountability, I decided to take on this new challenge with the IAF. Leaving the Centre was hard. I was a founder and led the organization for 13-years.

The foundation's focus will be on using values to reverse a trend I have seen over the past 15 years. Today, too many privacy programs are about completing bureaucratic tasks, such as writing purpose-specification notices or managing preferences. I believe we have seen a similar trend at many

enforcement agencies that have found it easier to measure technical compliance rather than compliance with the true purpose of data protection. Furthermore, I have also seen enforcement agencies struggle when they attempt to apply legacy enforcement concepts to new observational-based applications such as online and physical tracking, sensors and cameras. Compliance with technical requirements is important, but it is not sufficient. It is not why societies believe in privacy.

Privacy processes have always been about protecting the dignity of the individual and prevention of harm. To assure dignity and prevention of harm, early privacy laws went down two different roads. One road led to protection based on individual control. Individual control was predicated on minimal flows of data that came directly from the individual, with the individual granting limited usage rights based on a stated set of purposes. This pathway indirectly maintained dignity by assuring the individual's autonomy.

The second road was based on defined harms. Those harms were easily recognizable, like denied credit based on inaccurate data or reputational risks related to disclosure of video rentals. This second road makes sense if new information-related harms evolve slowly and legislators are able to identify those new harms in a timely manner and enact new laws quickly.

Waves of new technologies have marginalized the utility of both roads. Those new technologies began with database software in the 1970s and have included statistics, distributed processing, increased storage capacity, faster processing, easy-to-use open networks, mobile telephony, common processing modules, facial recognition, mobile computing and now Big Data. They have made data critical and obscured the individual's role in collection by the organization. New opportunities create new harms and risks to dignity, and many of those harms and risks are hard to measure with a calculator. Risks to individuals need to be mitigated at a pace that runs much faster than legislation.

> *"Today, too many privacy programs are about completing bureaucratic tasks, such as writing purpose-specification notices or managing preferences."*

Martin Abrams

The Information Age has brought incredible possibilities to our Earth. Personalized medicine, better vehicles, new social settings and better opportunities are its treasures. However, expansive data has marginalized data protection concepts that were based on individual control. To harvest the treasures, we must mitigate the risks.

So we return to the purposes of privacy protection. They are about dignity and prevention of harms that are constantly evolving. Our Digital Age requires data protection based on responsible organizations answerable to us, either individually or through enforcement agencies. This requires organizations having the willingness and capacity to understand how to recognize new risks related to data usage, proportional to their size and the risks they create for individuals and society.

This doesn't just mean behavioral changes at companies; it also means change in how regulators allocate time and resources. Lastly, the policy debate must move from control by individual to under control by users of the data; from individuals bearing the governance burden to that burden being carried by data users.

This challenge of evolving data protection requires an organization focused on the policy and infrastructure underpinning of accountability. It must include all stakeholders, and its work must be trusted. That was why the Information Accountability Foundation was founded, why I am taking the helm and why I would welcome your participation in this journey.