The Appropriate Use of Information

An Interview with Jennifer Barrett, Global Privacy Leader, Acxiom Corporation

Jennifer Barrett

EDITORS' NOTE *Jennifer Barrett joined Acxiom Corporation in 1974 after receiving a degree in mathematics and computer science from the University of Texas at Austin. Barrett serves on a variety of industry boards, including boards and councils of the Direct Marketing Association such as the Safe Harbor Ethics Committee and the DMA Political Action Committee. She is past Chair of the DMA Committee on Social Responsibility and sits on the executive committee of the Centre for Information Policy Leadership and the Information Policy Institute.*

COMPANY BRIEF *Founded in 1969 and headquartered in Little Rock, Arkansas, Acxiom Corporation (www.acxiom.com) is a global interactive marketing services company. Tailored for a wide range of industries and business needs, the company's products and services help the world's leading companies strengthen their relationships with existing customers and initiate relationships with new customers. Acxiom is a developer of some of the largest and most sophisticated business intelligence and marketing databases in the world, enabling clients to analyze their customer base, improve customer acquisition and retention, grow the value of customer relationships, reduce risk and protect against fraud, and manage large volumes of data.*

How do you define the role of Global Privacy Officer?

The role is evolving as the issue of privacy evolves. The role focuses on leading a company toward a culture of understanding the appropriate use of information for its business. As information permeates everything we do, the role is getting more complex and diverse each year. The appropriate use of information includes what you collect, where you collect it, what you do with it, and who you share it with. It has a dynamic of compliance because in some cases those activities are regulated by law. If you're a financial services or a health care institution, law dictates how you must treat certain kinds of information, and laws in different parts of the world are driven by cultural attitude and by how the government operates.

How challenging is it to have a consistent platform for rules and regulations, and does there need to be consistency?

Consistency may be too strong a word because we have to respect cultural and regional differences. A better word might be harmonization. There has to be some rationale about how information moves around the world. We've all got to understand and respect our country and our culture, but we also have to recognize that information flows globally. How can we respect our people while respecting other cultures' dynamics? For example, the law in Europe relative to using an e-mail address for marketing solicitation purposes requires opt-in; the law in the U.S. requires opt-out. We have to respect those differences, which is doable, but it's becoming cumbersome to comply with differing bureaucratic administrative procedures that neither create value for the consumer nor provide enhanced privacy protections because they often conflict with each other. Global Privacy Officers have been advocating that the place the data is collected sets the initial mark for whose laws apply. Then, as data moves around the world, those regulations are honored, and the data is appropriately protected from misuse.

Is it challenging to stay on top of the rapid changes in technology?

It's challenging because new technologies come on the scene every day. Many Global Privacy Officers are spending time promoting self-regulation and best practices because the laws that regulate what is an appropriate use of information are always behind the technology curve. New technology is great, but we have to ask ourselves what we should do with it and what should we not do with it even if we can. Just because it's legal or not regulated doesn't necessarily mean we should do it, especially if it will not build credibility in the marketplace or confidence with customers.

Are young people excited about opportunities in the industry?

There is a growing realization that this is an emerging field. I work with two different university-level programs to teach these concepts. We work with the computer science area because so many of the technologies are coming out of that area and also with an advanced marketing degree program because marketers want information to understand who their customers are, which is one of the data-rich areas of any business. There also is a group called the International Association of Privacy Professionals that was founded about five years ago. The first meeting I went to had about 150 people. I just attended an academy last week in Orlando, Florida, and the group has more than 5,000 members worldwide. I think its popularity speaks to people wanting knowledge and needing to build a network with other privacy professionals, as well as a desire for training, because the association offers a professional certification program. The privacy profession will emerge over the next decade as a far more important and thus recognized role. In some places in Europe and Asia, law requires that someone perform the job of thinking about these issues and making sure the company is using information appropriately.

Are there opportunities for women to grow into senior-level positions?

It's such a new job that I don't think there is any gender bias at the moment, and a lot of Privacy Officers are women. Most at the senior ranks got into it because they were recruited, not because they sought it out. Once it's better established, I think people will want to pursue it as a career.

What key areas of focus are in the forefront of your mind with regard to continued leadership and client fulfillment?

Information has no borders. Information can be at any moment in time almost anywhere, so we've got to elevate our thinking to some degree, even a little bit outside our comfort zone from a cultural standpoint. We've got to focus not only on privacy, but on security and safeguarding information as well. The privacy function and the security function walk arm and arm. You can have good security without having good privacy, but you can't have good privacy without having good security. ●