



## **Large Databases Bring Large Responsibility**

*Originally published in the DMNEWS on March 14, 2005*

Last week, while in Washington DC at an [IAPP](#) Privacy conference, I decided to head over to the Senate hearing on ID theft. The hearing was prompted by a number of recent events, including: the information breach at a division of Lexis-Nexis, the loss of several data tapes by Bank of America, and the emerging scandal at data-broker ChoicePoint. The line into the hearing room was long. In fact, it was so long that several people who had been waiting in line for hours found themselves unable to get into the hearing – myself included. Apparently, all this talk about new privacy legislation has gotten our attention.

DMA President John Greco was also in DC that day to address the conference of privacy professionals. Mr. Greco emphasized the DMA's focus upon the consumer, and noted today's consumers' desire to have greater control over his relationship with the companies (s)he patronizes. I certainly support the DMA's new philosophy, and am looking forward to seeing how this mantra plays out in light of recent events.

Historically speaking, large database companies have been free to operate with very little governmental oversight. Yes, there are laws that regulate the data that's used to compile consumer credit reports. But there are notable loopholes in much of that legislation. Case in point, if Social Security numbers, Federal Employer Identification Numbers, bankruptcies and lien information are not considered to be credit report data, then I'm not sure what would be.

Many of the privacy principles that we have in place were conceived in a much simpler time - a time prior to the onset of massive, relational databases. Back in 1970, lawmakers and policy experts could not have imagined our industry's current ability to collect, store and utilize enormous amounts of consumer data. And I'm not sure we as an industry have fully grasped those capabilities. In some ways, our eyes are bigger than our stomachs - our capacity for data has outpaced our ability to safeguard it.

Implicit in the concept of consumer control is the notion of having control over one's own data. If the direct marketing and data collection industries are truly going to offer greater control, some of us will need to make significant structural and cultural changes to the way we do business. If we are going to suggest that our industry has a right to maintain massive amounts of sensitive consumer data, then we need to take extraordinary measures to protect that data. With large databases goes large responsibility.

The true question is HOW to provide that control to consumers. At this point it is likely that one method will be to enact specific legislation. As I write this, Congress is

considering several bills which are modeled on California's SB 1386, and which require that companies notify consumers in the event of a data breach. In an era of consumer control, notification of a data breach should fall under best practices. And the idea that many companies have not and would not notify their customers of a breach without this legislation is troubling to say the least.

Moreover, there are more than a few state legislatures talking about enacting credit freeze laws, which would allow consumers to prevent companies from accessing their data for the purpose of providing them credit. Our industry has already been hit with do-not-call. We've withstood threats regarding do-not-email. Will we soon need to reckon with do-not-CollectMyData? Can you imagine the impact upon the direct marketing industry if even half of the 78 million who've signed up for the do-not-call list decide to take advantage of a national credit freeze law?

As marketers, we can all recognize how precious a commodity that data is. Personally, it absolutely kills me when I think about the number of companies that are NOT doing enough to use data effectively to enhance their customer experience. Data should be cherished. It should be protected. It is the absolute lifeblood of our industry. So whenever I read about a situation where a company is not able to keep their data secure, I cringe.

Why? Because it's hard enough already to get consumers to willingly provide marketers with their data. To take an active role in their relationship with companies. To open themselves up to forging a better, and more in depth relationship with the brands they trust.

Our industry has an opportunity to take a leadership role on these issues: by embracing legislation that puts the consumer in control; by acknowledging the tremendous responsibility inherent in the stewardship of our customer's personal information; and by going to extraordinary lengths to protect that data. These are heady challenges indeed. Our collective response to those challenges will impact our business for the next decade.

*Alan Chapell is president of Chapell & Associates, a consultancy focusing on privacy, marketing and consumer perceptions. He is the New York chapter co-chair of the International Association of Privacy Professionals, publishes a [daily blog](#) on issues of consumer privacy, and will be teaching a [class](#) on privacy and marketing at NYU this summer. His e-mail address is [achapell@chapellassociates.com](mailto:achapell@chapellassociates.com).*