New Jersey Law Journal

VOL. CXC– NO. 14 – INDEX 1183 DECEMBER 31, 2007 ESTABLISHED 1878

Commentary

Greater Data Security, and Cures For Abuse, Are Way Overdue

By Grayson Barber

When people disclose information about themselves to the government, their banks, their doctors or even strangers, they generally do not expect that the information will be re-disclosed, sold or published worldwide on the Internet. But it happens all the time.

Personal information has become a lucrative commodity, and the more intimate the better. Commercial data aggregators routinely mine government records to gather information about individuals. Financial institutions give information to their affiliates under the federal law known as Gramm-Leach-Bliley, and health care providers sell medical information to advertisers legally, through the Health Insurance Portability and Accountability Act (HIPAA).

Markets for personally identifiable information are thriving, but with hidden costs that are only just beginning to be recognized. Identity theft is the most obvious. There are others as well, which have emerged slowly because their impact has been felt by groups that are already marginalized.

For example, the way commercial databases are used, we are creating an underclass of people who have difficulty getting jobs, cannot get loans and for whom life is more expensive because of low credit scores. Data mining companies that perform employee background checks keep permanent records of arrests and criminal sentences that cannot be corrected or expunged. Minority groups are disproportionately represented in the vulnerable population of people who have such records.

Current laws, policies and practices fail to address the root causes of these systemic problems. Naturally, the parties with the greatest influence are those who benefit most from the status quo. In particular, companies that turn a profit from collecting and then selling personal information, often through open government records requests, have lobbied forcefully to ensure that public sources of private information remain open.

The remedy must begin with increased data security measures, data minimization and public education. To improve data security and reduce identity theft, organizations must internalize the cost of their data-collection practices.

To illustrate: identity theft is a crime of opportunity. Thieves seize the opportunity when individuals and organizations fail to safeguard personal information. To minimize the risk of identity theft, we need to increase data security measures, minimize data collection and inform the public by telling people when their personal information has been disclosed.

Individuals cannot cure the problem alone. We have no choice but to participate in commercial databases to get basic services in the community.

That is to say, the root of identity theft lies not with consumers or identity thieves, but with government and private agencies that collect and store excessive amounts of often unnecessary personal information in systems that lack adequate privacy and security safeguards. The misuse of stolen consumer information can be minimized by using specific identifiers instead of Social Security numbers and other "universal" identifiers.

Historically, this has been difficult. Companies have been reluctant to take extra security measures, which introduce inefficiencies and expense, especially so long as the consequences are borne not by them but by the consumers.

The agencies that collect personal information will have no incentive to minimize data collection or improve security until the agencies themselves bear the consequences of identity theft and other social costs.

Government agencies in particular should have a special obligation to ensure that personal information is not exploited to the detriment of citizens. At

Barber, a solo in Princeton, concentrates on privacy matters.

the very least, they should curtail the publicly available sources of Social Security numbers, including court files.

Congress has tried to limit the use of Social Security numbers as a de facto national identifier. The Privacy Act of 1974 made it unlawful for a government agency to deny a right, benefit or privilege because an individual refuses to disclose his or her Social Security number. Not until identity theft reached a crisis level, unfortunately, did the perils of using such numbers become widely recognized.

The other social costs, which are just as real, have yet to be similarly acknowledged. To remedy the situation, data custodians should be responsible for data security breaches.

The bench, the bar and the Legislature should be striving to ensure that personal information is treated in a manner that is legal and fair to the individuals who are affected. In addition to adopting fair information practices, we must craft meaningful remedies for individuals who are harmed by misuse of personal data, even when the data came from a "public" source. ■