Courts and Congress May Redefine Consumer Protections

By Harry A. Valetk
New York Law Journal

Information about us is everywhere: Addresses, telephone numbers, dates of birth, driver's license records, political-party affiliations, bank account numbers, and even Social Security numbers are readily available in the public domain.

Thanks to the freewheeling data exchange practices of insurance companies, telephone and utility companies, pharmacies, and commercial enterprises, personal data collection has flourished into a multimillion-dollar industry.

Fortunately, the quest to reclaim a basic sense of privacy has found new momentum in two significant recent events: a New Hampshire Supreme Court decision setting new standards for disclosing personal information and U.S. Senator Dianne Feinstein's (D-California) legislative initiative under the Privacy Act of 2003.

'Remsburg'

In *Remsburg v. Docusearch, Inc.*, the New Hampshire Supreme Court concluded in February that the family of a murdered young woman has grounds under state law to sue the information broker hired by the victim's stalker over the Internet to locate her.[1]

Remsburg began with the tragic 1999 murder of Amy Lynn Boyer, a 20-year-old woman from Nashua. Ms. Boyer died after her stalker, Liam Youens, shot her in cold blood as she left work, and then turned the gun on himself.

Mr. Youens used Docusearch, an Internet-based investigation and information service site operated by a private investigator in Florida, to find out everything he could about Ms. Boyer. In five separate transactions with Docusearch, amounting to $95 in fees, he obtained enough information to track her daily routine.

At first, Docusearch could not find Ms. Boyer's work address. But after repeated requests from Mr. Youens, Docusearch hired a subcontractor, who conned Ms. Boyer into revealing it. Eventually, Mr. Youens was able to obtain her home address, date of birth, Social Security number, and the location of the dentist office where she worked.

Recognizing the need to protect unsuspecting victims, the New Hampshire Supreme Court stated: "If a private investigator or

information broker's disclosure of information to a client creates a foreseeable risk of criminal misconduct against a third person whose information was disclosed, the investigator owes a duty to exercise reasonable care not to subject the third person to an unreasonable risk of harm."

In examining whether the threat of criminal misconduct is foreseeable, the court specifically looked at two increasing risks associated with typically lax disclosure practices: stalking and identity theft.

"The threats posed by stalking and identity theft lead us to conclude that the risk of criminal misconduct is sufficiently foreseeable so that an investigator has a duty to exercise reasonable care in disclosing a third person's personal information to a client. [T]his is especially true when, as in this case, the investigator does not know the client or the client's purpose in seeking the information."

Loosely Regulated Industry

The *Remsburg* decision comes at a time when private companies are collecting personal information on a massive scale.

In March, Italian clothing designer Benetton Group raised significant privacy concerns when it announced plans to weave radio frequency identification chips into its garments to track them around the world.[2]

Experts quickly warned that these chips could pose significant risks to consumer privacy because they would allow anyone with a radio frequency identification receiver to locate customers wearing Benetton clothing, including companies peddling their own products.

In response to mounting public concern, Benetton executives later announced that wireless transmitters would not be added to their garments anytime soon.[3]

Still, the menacing assault on consumer privacy remains. A vast majority of commercial Web sites collects personal information about visitors, and routinely exchanges it with third-party "business partners" to create profiles of consumer preferences.

Health care providers and insurance companies also swap sensitive patient data to predict costs; and supermarkets and pharmacies offering discounts to customers who enroll in special club card programs, which track buying patterns.

Perhaps most troubling of all is that exploiting these public information sources gets easier every day. For example, courts nationwide are now digitizing legal records historically found only in dusty cellars, and making them available online.

In Hamilton County, Ohio, the Clerk of the Court maintains a comprehensive Web site that has advanced name-search features on civil, criminal, and even parking violation cases freely available to anyone with Internet access.[4]

The site requires no password or user fee, and the database is alarmingly user-friendly. To find all of someone's available records, users simply search by name. Anyone can browse through detailed court records, and each file displays all publicly held information about a case — including Social Security numbers, home addresses, and financial disclosure forms.[5]

Another site, anybirthday.com, claims to have more than 135 million birth dates readily available to anyone with Internet access — and it's

absolutely free. All that is needed is the first and last name of the individual. For those willing to part with a $29 one-time annual fee, anybirthday.com will also disclose anyone's home address.

According to its privacy policy, the site's records are all derived from non-privileged public access information sources: "Information found in the anybirthday.com database can be found elsewhere by anyone with a simple knowledge of public record access."[6]

The lesson here: Personal information today is seldom private.

Privacy Act of 2003

To address the need for basic protection at the national level, Senator Feinstein last month introduced the Privacy Act of 2003 to stem the increasing number of identity theft cases and other privacy abuses within the information mining industry.[7]

If passed, the new law would establish a two-tiered system of protection for all personal information. Sensitive personal data, like Social Security numbers, would fall under an opt-in system, requiring companies to get an individual's express permission before the sale, licensing, or renting of the information to third parties.

Non-sensitive personal data, like names and addresses, would fall under an opt-out system, requiring businesses to give individuals the opportunity to withhold their personal information.

Other provisions of the bill include:

• Prohibiting businesses from denying service to anyone who refuses to disclose his or her Social Security number.

• Creating criminal penalties for ill-meaning individuals obtaining Social Security numbers to find and injure another person.

• Expanding the opt-in requirements for health data to include a number of institutions, including researchers, universities, and law enforcement officials.

• Closing loopholes in the Driver's Privacy Protection Act so motor vehicle departments will no longer be allowed to disclose sensitive information on licenses.

• Protecting personal information regardless of the medium through which it is collected.

Outlook on Privacy

To pave the way for the future, legislators must ensure that consumers are given more control over how their personal information is collected, used, and sold by private industry. To that end, privacy legislation at the national level defining consumer protections and identifying areas of merchant liability would be easier to comply with than varying state case law.

For its part, the information collection industry should take a closer look at current exchange practices, and figure out new ways to ensure disclosure is carried out responsibly.

Otherwise, assuming Congress fails to act soon, courts in other states, including New York, may soon adopt New Hampshire's "foreseeable risk" approach, and hold that personal information should be reasonably guarded and disclosed only with good cause.

Harry A. Valetk is an attorney with the U.S. Department of Justice in Manhattan who writes about identity theft, online child safety, privacy protections, spam scams, and cyberstalking laws. The opinions expressed here are the author's, and not those of the U.S. Government.

FootNotes:

[1] Remsburg v. Docusearch, Inc., 816 A.2d 1001 (N.H. Feb. 18, 2003).

[2] Elisa Batista, What Your Clothes Say About You, Wired News, http://www.wired.com/news/wireless/0,1382,58006,00.html (March 12, 2003).

[3] Elisa Batista, 'Step Back' for Wireless ID Tech?, Wired News, http://www.wired.com/news/wireless/0,1382,58385,00.html (April 8, 2003).

[4] Clerk of the Courts Web site, Hamilton County, Ohio, http://www.courtclerk.org (last visited on May 5, 2003).

[5] See Liz Sidoti, Revisiting Public Record Policies, CBSNews.com, Oct. 11, 2002, www.cbsnews.com/stories/2002/10/11/tech/main525358.shtml (last visited on May 5, 2003).

[6] Anybirthday.com Privacy Policy, http://anybirthday.com/privacy.htm (last visited on April 30, 2003).

[7] Privacy Act of 2003, S.745, 108th Cong. (2003).

Date Received: *May 12, 2003*