

## **Inside 1to1 Privacy**

**Date: 03/02/2009**

**Issue: March 2009**

**People: Don Peppers & Martha Rogers, Ph.D.**

### **Growing Use of Background Checks and DNA Databases Raises Policy Questions**

How much are we willing to intrude upon the privacy of innocent people in order to identify criminals? The answer across North America and Europe appears to be "quite a bit." A growing use of background checks at all levels of society and the emergence of DNA databases is testing the privacy boiling point for millions of people.

#### **Background reports in every office**

Background checks--once the province of large employers--are now de rigueur for the smallest organizations. Thanks to the popularization and affordability of online public databases such as Intelius, schools, places of worship, little leagues and other nonprofits are running background checks on parent volunteers.

One *Inside 1to1: Privacy* editorial board member reported witnessing a church in the UK run a background check on a Sunday school teacher. Another board member had his background checked when he coached youth soccer in New England, and a third had to submit to a background check in order to be a driver on a school field trip in the Midwest.

What is the common goal of these checks? To ferret out sexual predators and drunk drivers, say the organizations ordering them. Because of the potential catastrophic risks to children, parents in large part go along with these inspections into their personal lives.

But what risks are these parents accepting? The most important may be a heightened vulnerability to identity fraud. The small organizations conducting the background checks typically employ unsophisticated methods for collecting, storing, transmitting, and discarding these highly sensitive documents. Most, for example, require parents to complete hand-written forms that are mailed or faxed, and then stored indefinitely in easily accessible cabinet drawers. A break-in at any small organization has now become a potential privacy exposure for hundreds of people.

Another downside is the awkward position parents find themselves in with respect to

church and school secretaries, who potentially have access to the background reports.

### **DNA databases in every jurisdiction**

The growing effectiveness of using DNA evidence to secure criminal convictions has spawned a new platform for ubiquitous identification: the DNA database. The popularity of these repositories--once limited to DNA sequences of people convicted of serious crimes--has emboldened many jurisdictions to expand their reach to people merely arrested.

The UK Home Office claims it created in 1995 the world's first DNA database, the National Criminal Intelligence DNA Database (NDNAD). *The Register* reported last November that NDNAD contains more than five million genetic profiles--roughly eight percent of the UK's 60 million population--including "up to a third" from people who were never convicted of a crime. Indeed, the European court of human rights ruled in December that NDNAD, in keeping innocent people's DNA records in a criminal register, breached Article eight of the Human Rights Convention.

For its part, the FBI's Combined DNA Index System (CODIS) reportedly contains more than 6.4 million offender profiles. Among U.S. states, each maintains its own DNA database, with California hosting the third-largest in the world, behind the NDNAD and CODIS. Thirty-four states record DNA for convicted misdemeanors, and 11 states retain data on those arrested for murder and sexual crimes. Some law-enforcement backers have advocated storing DNA on every American in order to improve prosecution of first-time criminals.

"This is the single best way to catch bad guys and keep them off the street," Chris Asplen, former executive director of the National Commission on the Future of DNA Evidence, told the Washington Post.

What are the privacy risks of the proliferation of DNA databases? Privacy advocates say our overconfidence in the reliability of DNA evidence could link innocent people with crime scenes in ways that are hard to disprove.

This risk could be increased with greater cross-jurisdictional data sharing. The U.S. and UK have sought through the "Server in the Sky" initiative to link their DNA databases with Canada's National DNA Data Bank and their counterparts in Australia and New Zealand.

The prospect of every person's DNA ending up in a database is becoming a reality in some jurisdictions. In addition to criminal DNA databases, several government health

agencies maintain DNA databases for disease identification and prevention. The State of Minnesota, for example, retains DNA from all newborns to perform genetic screening.

### **Policy questions**

Citizens in Western democracies will continue to demand effective crime prevention and prosecution using the latest available technologies such as background checks and DNA databases. But the expansion of these practices to envelop higher numbers of innocent people will inevitably result in more privacy exposures and erroneous imprisonments.

How can the organizations using these screening methods minimize their privacy impact? Hugo Teufel, outgoing CPO of the U.S. Department of Homeland Security, answered that during a January address in St. Paul: "fair information principles, you'll always come out with the right answer."

What would those principles prescribe for background checks and DNA databases?

- Notice. Individuals whose data could be captured or screened would be conspicuously informed ahead of time.
- Choice. Individuals can easily opt out of non-essential systems such as health-screening databases.
- Use and Retention Limitation. Background check and DNA data can only be used for the screening purpose, and not merged with other unrelated systems. Data on innocent people must be de-identified once innocence is established.
- Access. Individuals must be able to review and submit corrections for their data kept on file.
- Security. Because of the high sensitivity of the data involved, these systems must employ the highest available security.

Without a strict adherence to internationally recognized privacy principles, the growing ubiquity of population-screening measures risks a public backlash that could eventually undermine their continued support.