KLAAS ACTION REVIEW

THE NEWSLETTER OF THE MARC KLAAS FOUNDATION FOR CHILDREN

A MESSAGE FROM MARC

In 1996, the KlaasKids Foundation engaged in the privacy debate by exposing the multi-billion dollar Direct Marketing Association's (DMA) practice of indiscriminately selling children's private information. Although our Kid's Off Lists legislative campaign proved unsuccessful, a high-profile news story—by a reporter who used the name of Polly's killer to purchase children's private and identifying information—helped induce the DMA into establishing voluntary privacy regulations. Those events and a successful class action suit against list provider RR Donnelley have prompted this issue of the *Klaas Action Review,* focused entirely on privacy matters.

While the *Review* will remain in production, this is the last hard-copy issue that will be printed. For budgetary reasons, we are following in the footsteps of many other organizations and switching to a fully electronic format. The *Review* will continue to be available via email and through our website at www.klaaskids.org, providing news, updates, and commentary on our ongoing campaign to improve child safety. If you would like to receive a PDF version of each newsletter, please send us your email address.

We also invite your tax-deductible contributions to help us carry on this important work. The KlaasKids Foundation functions entirely on the monetary and in-kind donations of its many wonderful supporters. Our readers are aware of our many achievements over the past few years: key support for several important pieces of legislation dealing with such issues as sex offender registration, state accountability for paroled criminals, child information privacy, and stopping criminals from selling memorabilia; support for programs such as CARE Alert, Team HOPE, and DNA databases; providing new resources to families such as the Child Safety ID Kit and a missing child resource guide; sending speakers around the country; and much more. All this has been possible because of your support and help. We ask you to continue participating in this vital effort.

Privacy Today

Today, our work is more important than ever. Public safety concerns regarding privacy were ignited in the aftermath of the Twin Tower and Pentagon tragedies. Scientific and technological advancements

(Continued on page 7)

INSIDE

Are You Feeling Private Today?

By Mary Freeman

Ever since 9/11, we've heard time and again that "everything has changed." Most people believe that this is particularly true when it comes to the privacy of their information. In a society where consumers have increasingly feared for the privacy of their personal data for the past several years, it is assumed that almost anyone can today use the Internet to access every kind of information about individuals' lives, families, finances, personal addresses and phone numbers, and product preferences. It is also believed that the government will now be digging ever more deeply into private records in its struggle against terrorism. But is our privacy situation really as bad as that?

The fact of the matter is that most information is about as safe as it ever was, offline or on.... the media's focus on hacker attacks has caused much more suspicion than is actually warranted.

What Are We Afraid Of?

According to a 2000 study, "Public Attitudes Toward Uses of Criminal History Information," by Dr. Alan F. Westin of Columbia University, misuse of personal information is a major concern to the general public today. "Nearly 90% of adult Americans are concerned about the possible misuse of personal information, with 64% expressing a high level of concern," the report states. Thirty-eight percent of Americans have felt victimized by businesses collecting and using information; political groups or nonprofits; law enforcement agencies; or government organizations.

Unfortunately, according to the same report, many myths are also being perpetuated in the Internet age:

- 52% percent of adults believe that anyone's credit report is available online.
- 49% believe that anyone's criminal conviction record may be purchased via the Internet.
- 36% believe that bank balances are for sale online.
- Approximately 4 in 10 adults believe that they can obtain anyone's Social Security number (42%), credit card number (39%), or arrest record (38%).

Fortunately, these beliefs are largely false.

Applying Common Sense

The fact of the matter is that most information is about as safe as it ever was, offline or on. Steve Hunt, vice president of security research at Giga Information Group, said in a recent interview that the media's focus on hacker attacks has caused much more suspicion among consumers than is actually warranted. "We have willingly surrendered privacy for years," he commented. "Why do we care now?" He believes most consumers mistakenly think that the Internet makes privacy violation far easier.

It is true that an experienced hacker can gain access to Social Security numbers or credit card information if sufficiently motivated. The odds of it happening to you are about the same as a thief breaking into your home or stealing your purse. However, the average consumer is not greatly at risk in a hacker attack. In the hacker culture, it is the thrill of breaking into tightly secured systems, not deliberate theft, that is usually the goal. Financial losses in such cases, if any, are the responsibility of the entity being attacked.

Identity theft has also garnered a great deal of public attention, not because it is frequent, but because of the upheaval it creates for the victim. Most of this is due to improper notification of credit companies, and some very sloppy identification systems still present in state-level Departments of Motor Vehicles. Better legislation is needed to improve these systems and strengthen defenses for consumers. However, identity theft rarely takes place because of online activity. Usually, it is based on a stolen driver's license.

The fact is that the vast

percentage of all crimes still take place the old-fashioned way: through physical invasion, observation, and attack. Consumers can protect themselves and their families online by using basic common sense—not giving out personal information on websites or to chatroom buddies (see below), avoiding websites which ask you to fill out information forms or to register, and calling in credit card numbers instead of sending them online. By far, the greatest personal information sharers remain your bank, credit card companies, and direct mail list vendors.

Tighter Government Surveillance

More attention has been brought to privacy issues since the 9/11 attack, thanks to nearly a dozen Internet security bills which have been introduced into Congress. Perhaps the most notorious is the Cyber Security Enhancement Act of 2001, sponsored by Representative Lamar Smith. This bill would allow the government to request subscriber information and copies of email from Internet Service Providers (ISPs).

Some tightening of Internet standards seems inevitable, in light of the discovery that much of the 9/11 attack was planned using the Internet. However, such permissions do not currently affect the average citizen who sends email, maintains a website, shops, or runs a business online. Government investigations are aimed at groups and fundraising organizations suspected of involvement with terrorism.

Privacy Foundation fellow Philip L. Gordon predicts that as time passes, the pendulum will swing back toward dealing with consumer concerns about privacy rather than security, revealing that underlying circumstances have not changed, according to NewsFactor Network. "You still have a tremendous need on the part of individuals to give up part of their information in their day-to-day lives to get the products and services they want," Gordon said.

In some cases, privacy should actually improve in the coming months. The FTC has cracked down on marketers making fraudulent claims via junk email and telemarketing, and is working on a national "do not call" list to protect consumers from phone sales pitches. ■

The Children's Online Privacy Protection Act

By Parry Aftab

The recently enacted Children's Online Privacy Protection Act (COPPA) is a federal law that requires websites to get permission from parents before the sites are allowed to collect personal information from children or allow them to use interactive features like email, instant messaging, chat, and message boards. In part, the COPPA was designed to protect kids from overreaching marketers who attempt to access social security numbers to where you invest your money before letting them play cool online games. However, it is also a tool to alert parents when children are involved in activities that allow them to communicate with strangers, who may not be what they appear.

Our kids are so trusting, they will often reveal their names, addresses, phone numbers or other personal or identifying information to online "friends" who may only be masquerading as children.

Under the law, control over online use is put firmly in the hands of parents. If your kids go to websites that offer interactive features or have registration, you will probably find an email from the site in your own email box. The email will tell you that you need to give consent for your child to participate, and that you should read the site's privacy policy before you consent.

The best advice I can give you is READ THE PRIVACY POLICY. That's the only way you'll be able to tell if the site offers an environment you think is safe and appropriate.

For example, there are many models for chat that a site can offer: completely unmoderated, where everyone can discuss anything and everything; moderated, so that discussions are supposed to be kept on track (and in those cases, look at who the moderators are: Responsible grown-ups? Fellow kids?); private chats, where kids can only chat with people you put on their "friends" or "buddy" list; etc.

If the policy doesn't tell you everything you want to know, contact the website directly (the law requires that the sites include their email address, telephone number and mailing address in their privacy policies).

Parents know best what's right for their children. Reading the privacy policies gives you the information you need to make an informed decision about which online playgrounds your children will be allowed in. ■

Supreme Court Reviews Predator Registration

By Suzanne D. DiNubile, J.D.

Public notification of sex offender release has been in place as a national law for almost a decade. In 1994, the Jacob Wetterling Crimes Against Children and Sexually Violent Offender Registration Act was enacted. This Act required all states to establish registration programs for sex offenders by September 1997. The law is designed to protect children and was named after Jacob Wetterling, an eleven-year-old boy who was kidnapped in October 1989. Megan's Law, the first amendment to the Jacob Wetterling Crimes Against Children and Sexually Violent Offenders Act, was passed in October 1996. Megan's Law mandated all states to develop notification protocols that allow public access to information about sex offenders in the community. Megan's Law was named after Megan Kanka, a seven-year-old girl who was raped and murdered by a twice-convicted child molester living in her New Jersey neighborhood.

However, these laws have not been easily accepted by our society, and continue to face challenge after challenge in court. Courts also often dissent from each other in determining the constitutionality of such laws. Now, the Supreme Court is preparing to review these issues.

U.S. Supreme Court to Review State Decisions

On February 19, 2002, the U.S. Supreme Court announced that it will review the Ninth Circuit Court of Appeals decision which struck down the Alaska Sex Offender Registration Statute, on the grounds that it violated the Ex Post Facto Clause of the Constitution (which prevents a state from increasing the punishment for a crime after the crime is committed). States are able to place restrictions on a defendant after the crime is committed and time is served as long as they are not punitive. With Megan's Law, the Ex Post Facto issue is whether an offender whose offense was committed prior to the enactment of the statute should be subject to the statute.

The Ninth Circuit held that the Alaska statute is punitive and thus violates the Ex Post Facto Clause. However, the Tenth Circuit held that the Utah statute is not punitive.

The Tenth Circuit Court noted that Internet notification represents merely a technological extension, not a sea change, in our nation's long history. It makes information public regarding criminal offenses, and the farther removed one is from a sex offender's community, the less likely one will be to have an interest in accessing the particular registry.

In contrast, the Ninth Circuit concluded that the Internet does not limit its dissemination to those to whom the particular offender may be of concern, so it is beyond that which is necessary to promote public safety. Also, by broadcasting the information about all past sex offenders, the Internet exposes all registrants to worldwide ostracism that damages them personally and professionally and could make it impossible for the offender to find housing or employment.

One factor considered in determining whether a law is punitive is if it has historically been used as means of punishment. The Tenth, Ninth, Sixth, Third, and Second Circuit Courts have rejected the pedophile's analogy to shaming practices in Colonial times, because those practices, unlike Megan's Law, inflicted physical punishment. The person was either physically held up before his fellow citizens for shaming, or physically removed from the community.

The Ninth Circuit stated that the law amounted to punishment, since offenders must re-register four times per year for the rest of their lives and cannot escape the Act's grasp, no matter how demonstrable it may be that they pose no future risk to anyone. The court noted that with the exception of the Tenth Circuit, every sex offender registration and notification law that has been upheld by a Federal Courts of Appeals has tailored the provisions of the statute to the risk posed by the offender.

However, the Tenth Circuit rejected this analysis, stating that although other states have chosen to incorporate more defined risk assessment mechanisms, a statute is not necessarily punitive because a state has not achieved a perfect fit between ends and means. Thus, the considerable assistance Internet notification will offer in the prevention, avoidance and investigation of these serious and damaging crimes justifies the means employed.

The Right to Privacy and Due Process

The U.S. District Court for the District of New Jersey ruled on Dec. 6, 2001, that the disclosure of convicted sex offenders' home addresses on the Internet violates their constitutional right to privacy. In finding that the registry violated the sex-offenders' privacy rights with respect to their home addresses, the court relied on the Paul P. cases, which examined similar law and concluded that

"registrants possess a 'non-trivial' privacy interest in the confidentiality of their precise home address which is entitled to constitutional protection."

The court also held that the disclosure of the other information about sex offenders in the registry is not subject to a constitutional privacy right. The Court of Appeals for the Ninth Circuit had upheld Washington state's version of Megan's Law against a similar claim, in which plaintiffs failed to demonstrate the existence of a legitimate privacy interest in preventing the compilation and dissemination of truthful information that is already, albeit less conveniently, a matter of public record.

The Hawaii Supreme Court held in November 2001 that the Internet notification provisions of the Hawaii Statute violated the Due Process Clause of the Hawaii Constitution. This was because the statute did not allow for notice and a hearing in which the sex offender is given a meaningful opportunity to argue that he does not represent a threat to the community before disseminating the information on the Internet.

Reasons for Preserving Megan's Law

Every state in the U.S. has now enacted a version of Megan's Law. The objective is to limit recidivism by alerting the public to potential threats to public safety posed by convicted sex offenders. The universal adoption of sex offenders' registration laws reflects the importance of the interests they serve and the states belief in their efficacy. Approximately 30 states have already made registration and notification information available on the Internet. The Supreme Court should decide that the Alaska Statute does not violate the Ex Post Facto Clause. The Court should give guidance in its decision so that lower courts can identify any constitutionally problematic provisions and leave the rest of the states' registration and notification schemes in place.

The Tenth Circuit's decision is correct. Internet access to already available public information is merely an efficient way to organize and disseminate the important information needed to protect a community.

Those opposed to Megan's Law raise the concern of vigilantism. This is a minor issue compared to the violence that takes place against children when this information is not disseminated. Moreover, there is a caveat in bold type along with the information on each web site stating that the information should not be used to harass an offender and there are severe penalties for doing so.

Any ostracism and scorn felt by a sex offender stems only from his own shame about the act or acts he has committed. As the Third Circuit stated, "the sting' results from the dissemination of accurate public record information about their past criminal activities." If this shame is such an obstacle in a sex offender's life, he should seek psychological counseling, as his victims must if they expect to lead a normal life. There is no obligation for the state to keep public information inaccessible just to prevent a sex offender from feeling victimized.

Insofar as employment is concerned, it is up to particular employers who they want to hire. If the choice is between a non-sex offender or a sex offender, employers are entitled to information to determine the best candidates. If the job involves working with children in any capacity, there is a tremendous state interest in having the information readily available.

The Power of the Internet

The Internet provides an opportunity for great advancement in the protection of the children of America. Technology has added greater efficiency to the notification scheme with very little cost. The Utah statute, for example, was motivated by a request to quickly check approximately 100,000 volunteers submitted by the Boy Scouts. In the fast-paced and nomadic communities we live in today, technology provides good citizens with a tool to help protect children. In addition, the registration and notification requirement scheme facilitates a widespread deterrent against sex crimes, since offenders presumably do not want the information disseminated.

Law enforcement must keep up with technology in order to stay ahead of the offenders. It has recently been reported that the Internet is to blame for a boom in child sex abuse. Information technology is exploding and if the "information superhighway" cannot be used to help stop crime and protect our children, but only can be used as a tool to facilitate crime, our children are in grave danger.

Opponents of Internet notification argue that it could foster a false sense of security. In other words, if a young family figures all the potential offenders in the community are listed on a web page, they may let their guard down around dangerous people not listed on the site, assuming they are safe. This only emphasizes the fact that we must educate and promote community awareness along with registration and notification.

In addition, there should be severe and uniform penalties for non-compliance. This way offenders will be diligent in registering and will not be inclined to retreat to a state that is softer on sex offenders. ■

The Face of Evil: Technology Against Terror

By Joe Diamond

Since September 11, much attention has focused on "biometric" technologies as a way of improving the nation's security. Biometrics are computerized methods of identifying people based on physical or behavioral traits, including face recognition and voice analysis. "Biometric technology operates much like the gadgets in spy flicks such as *Mission: Impossible*—computerized scanners that confirm a person's identity by examining a biological feature, then match it with a digital file containing those exact characteristics," writes *Wired* magazine. "Identifiable traits can be physical, such as hand contours or retina patterns. They can be behavioral, such as voice modulation or keystroke typing rhythms.. [other] features being tested for singularity. include knuckle creases, body odors, even acoustic head resonances."

How Does It Work?

Face recognition in particular may hold great promise as both a tool against terrorists and more run-of-the-mill criminals. In some American airports, surveillance cameras are already hooked up so that if they scan the face of a suspected terrorist, a computer instantly alerts authorities. Similarly, a face recognition system trained on a schoolyard could warn police and school security of the presence of a sexual predator registered under Megan's Law.

Face recognition technology became widespread in Great Britain following a terrorist attack there in 1993. Among the benefits have been reductions in crime resulting from the "scarecrow" effect; criminals believe they are being watched and are more reluctant to act.

What About the Right to Privacy?

A Harris Poll of Americans after the September 11 attacks showed that 86% of Americans favor the use of face recognition technology to scan for suspected terrorists. Despite the concerns of civil libertarians, there is nothing unconstitutional about this technology. It is perfectly legal for the government to maintain a database with photos of suspected terrorists. Also, a person's right to privacy is limited when he's out in public, particularly in a transportation facility like an airport or bus terminal. Finally, the right to privacy does not mean a right to anonymity, and anyone who chooses to participate in a public activity like traveling by train or plane is by definition not anonymous.

As with any law-enforcement tool in a democracy, face recognition has to be used in a reasonable manner. But in general, the use of face recognition systems presents no legal issues that would ban its implementation, and the thoughtful deployment of this technology can play an important role in protecting the nation.

So far, at least, we know that face recognition systems will not catch every terrorist. John Woodward, a former CIA operations officer and now senior policy analyst with the think-tank RAND, notes that "facial recognition systems are not relied upon to make final determinations of a person's identity. Rather, the system alerts the authorities so that additional screening and investigation can take place. And though the system will make false matches that will subject innocent passengers to additional questioning and scrutiny, the current system routinely does the same."

Moving Toward Biometrics Use

Even if the technology at this stage is effective enough to catch (or deter) one potential terrorist, it should be deployed without hesitation. Biometrics firms will continue to refine face recognition, but only if airports and other customers provide funds for research and development. My organization, the Center for the Community Interest, is working with the KlaasKids Foundation and others to ensure that this does not happen.

We've drafted a resolution that calls for the continuing development and deployment of face recognition systems. It reads in part: "Face recognition technology can serve as a vital component of a comprehensive public security framework. Therefore, be it resolved that we the undersigned encourage America's local, state, and federal governments to deploy face recognition technology in airports and other vital facilities where the technology can be an effective weapon against and deterrent to terrorism and other forms of crime."

I invite you to read the complete resolution and add your name to it at www.communityinterest.org/resolution.htm. If you don't have Web access, please call me at 212-909-2620 and I will mail or fax it. ■

Joe Diamond is the public affairs director of the Center for the Community Interest (www.communityinterest.org).

Message from Marc (cont. from page 1)

previously considered threatening to personal safety are now accepted as the first line of defense against foreign and domestic terrorism. DNA profiling, biometric recognition technologies that match scanned biological features with databases of known terrorists and criminals, and websites that identify and locate registered sex offenders are just a few of the applications currently employed in the name of safe streets.

DNA Profiling

Because of its intrusive nature, DNA profiling may be the most controversial of the ultramodern crime fighting applications. In response to concerns and court challenges that non-voluntary DNA collection invades an individual's privacy or that collected materials might be used as a springboard for genetic engineering, legislatures have enacted special protections limiting the scope of DNA profiling to criminal investigations and identification. The fundamental building block for an individual's genetic makeup, a person's DNA is the same in every cell, and except for identical twins, no two individuals share the exact same DNA. Like fingerprints, DNA samples can be compared to known databases for identification purposes to solve crime, link crimes, or identify human remains.

Solving Cold Cases with DNA

In 1994, the U.S. DNA Identification Act mandated that the FBI establish the Combined DNA Index System (CODIS) database that enables local, state, and federal law enforcement to electronically exchange and compare DNA profiles.

As of 2002, 39 states participate in CODIS and its mission of linking unsolved crimes to each other and to convicted offenders. The potential for solving cold cases is enormous. California alone has an estimated 20,000 unsolved sexual assault cases in which biological evidence was obtained but never analyzed for the presence of DNA. While most state DNA cold case databases limit the collection of DNA samples to convicted violent offenders, there is increasing support to expand the population of inmates from which DNA can be extracted to include all convicted felons.

Prior to being convicted of sexually assaulting and murdering four women in Richmond, Virginia, in the mid-1980s, Timothy Spencer, the notorious "Southside Strangler," had previous convictions for burglary and trespassing. In response, in 1989, the state of Virginia legislated that offenders convicted of any felony in Virginia must submit DNA samples for the purpose of solving cold cases. As of December 20, 2001, Virginia had solved 584 cases through cold hits. One trend noted by analysts of the expanded cold hit DNA databank has been burglars who become sexual offenders, making it important to add DNA samples from all convicted felons to the database.

In Great Britain, authorities have been sampling DNA from individuals arrested for all recordable, violent and non-violent, offenses since 1995. Thus far, they have made 6,032 identifications: 4,461 offender-to-scene and 1,571 scene-to-scene matches.

Should We Do It?

If the states fail to duplicate the Virginia and British cold hit DNA models of profiling every felony conviction, America's law enforcement community will be severely limited in its ability to link and solve cold cases. Transient violent offenders will receive a free pass; we shall continue to release predators back into society and we will not allow victim families the resolution they need to move on with their lives.

The benefits of DNA profiling are manifest: The guilty will be held accountable and those falsely accused will be exonerated. Previously unrelated crimes can be linked to each other and to specific offenders. Unidentified bodies can be matched to missing person cases and resolution can be found for countless American families.

DNA is our most personal and private possession, for it defines our individuality. Therefore, whenever we are forced to involuntarily relinquish DNA, a specific framework must explain its scope and range. As long as DNA profiling is utilized as genetic fingerprinting to aid in criminal investigation and identification, it will be a powerful weapon in the war against domestic and foreign terror. However, if criminal justice DNA databases are utilized for genetic experimentation or typing, we will not only betray our own privacy, but we shall contravene our moral obligation to protect the sanctity of the individual. Then our pursuit of truth becomes an excuse to pursue a course of action that history continually reminds us is a recipe for disaster.■

Join the Foundation and Help Fight Crime!

To join the KlaasKids Foundation, please fill out this form and return it to the address below. Your tax-deductible membership costs just $15.00 per year, and includes an electronic subscription to the quarterly *Klaas Action Review,* with news and information, practical tips, events, and more.

Members may also receive:

- ❑ Information on starting a National Community Empowerment program.
- ❑ Safety information for your children.
- ❑ Information about how to support legislation against crime in your state.
- ❑ Other: _____

As a personal gift, you will also receive the Children's Identification Packet and a beautiful "Polly, We Love You" pin, in memory of our inspiration, Polly Klaas.

Name: _____

Address: _____

_____

_____

❑ Enclosed please find my tax-deductible donation of $_____.

❑ Discover Card ❑ Visa ❑ MasterCard

Credit card number is: _____

Expiration date: _____

Be sure to check out our website at www.klaaskids.org for regular updates and information on child safety. Give us your feedback!

KLAAS FOUNDATION FOR CHILDREN

KlaasKids Foundation
P. O. Box 925
Sausalito, CA 94966

Nonprofit
Organization
U.S. Postage
PAID
GMS