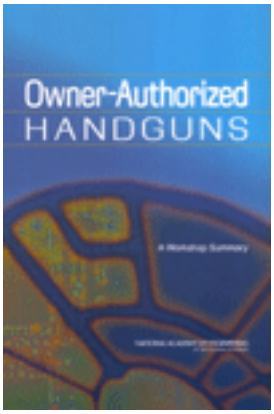

Owner-Authorized Handguns: A Workshop Summary

Lance A. Davis and Greg Pearson, Editors, Steering Committee for NAE Workshop on User-Authorized Handguns, National Academy of Engineering

ISBN: 0-309-52608-6, 68 pages, 6 x 9, (2003)

Owner-Authorized HANDGUNS

A Workshop Summary

Lance A. Davis and Greg Pearson, Editors

NATIONAL ACADEMY OF ENGINEERING
OF THE NATIONAL ACADEMIES

The National Academies Press
Washington, D.C.
www.nap.edu

THE NATIONAL ACADEMIES PRESS 500 Fifth Street, N.W. Washington, DC 20001

NOTICE: The project that is the subject of this report was approved by the Governing Board of the National Research Council, whose members are drawn from the councils of the National Academy of Sciences, the National Academy of Engineering, and the Institute of Medicine. The members of the committee responsible for the report were chosen for their special competences and with regard for appropriate balance.

Funding for the activity that led to this publication was provided by the National Academy of Engineering Fund.

International Standard Book Number 0-309-08975-1 (Book)
International Standard Book Number 0-309-52609-4 (PDF)

Additional copies of this report are available from the National Academies Press, 500 Fifth Street, N.W., Lockbox 285, Washington, DC 20055; (800) 624-6242 or (202) 334-3313 (in the Washington metropolitan area); Internet, http://www.nap.edu.

Printed in the United States of America

THE NATIONAL ACADEMIES

Advisers to the Nation on Science, Engineering, and Medicine

The **National Academy of Sciences** is a private, nonprofit, self-perpetuating society of distinguished scholars engaged in scientific and engineering research, dedicated to the furtherance of science and technology and to their use for the general welfare. Upon the authority of the charter granted to it by the Congress in 1863, the Academy has a mandate that requires it to advise the federal government on scientific and technical matters. Dr. Bruce M. Alberts is president of the National Academy of Sciences.

The **National Academy of Engineering** was established in 1964, under the charter of the National Academy of Sciences, as a parallel organization of outstanding engineers. It is autonomous in its administration and in the selection of its members, sharing with the National Academy of Sciences the responsibility for advising the federal government. The National Academy of Engineering also sponsors engineering programs aimed at meeting national needs, encourages education and research, and recognizes the superior achievements of engineers. Dr. Wm. A. Wulf is president of the National Academy of Engineering.

The **Institute of Medicine** was established in 1970 by the National Academy of Sciences to secure the services of eminent members of appropriate professions in the examination of policy matters pertaining to the health of the public. The Institute acts under the responsibility given to the National Academy of Sciences by its congressional charter to be an adviser to the federal government and, upon its own initiative, to identify issues of medical care, research, and education. Dr. Harvey V. Fineberg is president of the Institute of Medicine.

The **National Research Council** was organized by the National Academy of Sciences in 1916 to associate the broad community of science and technology with the Academy's purposes of furthering knowledge and advising the federal government. Functioning in accordance with general policies determined by the Academy, the Council has become the principal operating agency of both the National Academy of Sciences and the National Academy of Engineering in providing services to the government, the public, and the scientific and engineering communities. The Council is administered jointly by both Academies and the Institute of Medicine. Dr. Bruce M. Alberts and Dr. Wm. A. Wulf are chair and vice chair, respectively, of the National Research Council.

www.national-academies.org

STEERING COMMITTEE FOR NAE WORKSHOP ON USER-AUTHORIZED HAND GUNS

LANCE DAVIS, *Chair*, National Academy of Engineering, Washington, D.C.
MARK BEHRENS, ESQ., Shook, Hardy & Bacon, L.L.P., Washington, D.C.
PHILIP J. COOK, Duke University, Durham, North Carolina
T. DIXON DUDDERAR, Lucent Technologies (emeritus), Chatham, New Jersey
CHARLES F. WELLFORD, University of Maryland, College Park, Maryland

Project Staff

GREG PEARSON, Study Director and Program Officer, National Academy of Engineering
RAYMOND A. NASH, JR., Consultant
ROBERT CHERRY, NAE Fellow, Idaho National Engineering and Environmental Laboratory
CAROL R. ARENBERG, Editor, National Academy of Engineering

Preface

On June 2, 2002, the National Academy of Engineering (NAE) convened a one-day workshop to consider issues related to the development of owner-authorized handguns—firearms that would operate only for an authorized user. Nearly 40 individuals representing diverse organizations and perspectives attended the session. The workshop explored the technical feasibility, legal implications, and possible societal consequences of handguns engineered to prevent or reduce unintentional discharge or intentional, illegal use. The project was funded by the NAE and is consistent with the Academy's interest in topics that lie at the intersection of technology and society. The planning of the workshop and the preparation of the summary report were substantially aided by the volunteer services of the workshop steering committee. This report summarizes the presentations of invited speakers and panelists.

Lance Davis
Steering Committee Chair and
Executive Officer
National Academy of Engineering

Contents

Overview

On June 2, 2002, the National Academy of Engineering (NAE) convened a group of individuals in Washington, D.C., to discuss owner-authorized handguns. Some 40 people with diverse backgrounds took part in the one-day workshop (see Appendix A). This report is a summary of the workshop discussions, which focused on three topics: the state of the art of technology for creating owner-authorized handguns, liability concerns affecting the development and use of such firearms, and the potential impact of these devices on health and crime in the United States (see Appendix B).

The National Academies, of which NAE is a part, are accustomed to examining complex—sometimes controversial—issues at the intersection of science, technology, and society. Owner-authorized handguns, often called "smart" guns, have generated considerable public interest. The feasibility and utility of smart firearms have been debated in a variety of forums, but, for the most part, these discussions have not included the engineering community.

The June workshop, funded by NAE, was intended to set the stage for a more in-depth examination of owner-authorized handguns. In December 2002, NAE received support from the David and Lucile Packard Foundation to assess the technical feasibility of developing a reliable smart handgun. The 12-month project, which began in summer 2003, will provide

cost and time estimates for bringing one or more smart-gun technologies to the marketplace.

For the purposes of the June 2002 workshop, an "owner-authorized handgun" was defined as a firearm that would only function when operated by the designated owner of the handgun. In retrospect, a better descriptor might have been "user-authorized," since there are situations in which a person other than the handgun owner might have a legitimate need to fire the weapon. For example, more than one adult in a family might need access to a handgun for purposes of home-defense; and in some police departments, law enforcement personnel share firearms.

Whatever the terminology, owner-authorized handguns are meant to prevent specific unintended or undesirable uses of handguns: accidental shootings, usually by very young children; the shooting of police officers by assailants using the officers' own weapons; suicides, especially by teenagers; homicides by individuals using stolen handguns, guns purchased informally ("gray market" firearms), or guns sold illegally ("black market" firearms); and other crimes, including robberies, committed with stolen handguns or guns purchased on the gray or black market.

Simple methods of preventing guns from firing, such as grip safeties, have been available for a century or more. Although the focus of the workshop was on high-tech approaches to preventing unauthorized use, the application of certain low-tech solutions, such as trigger locks, could be an effective deterrent in some situations. More sophisticated technologies have only recently begun to be investigated. These include systems with electronic, magnetic, mechanical, radio, and sensor components, often in combination. Access may be controlled based on something the gun owner knows (e.g., a PIN code), something the owner possesses (e.g., a magnetic ring), or something unique to the owner (e.g., a fingerprint).

As is true of technologies generally, whatever technology is contemplated for owner-authorized handguns will be imperfect. Every technology has advantages and drawbacks and creates new, unanticipated problems. No single technological approach is likely to satisfy the needs of all handgun users. Police officers, for example, have different requirements for handguns than typical homeowners trying to protect their families. By the same token, the needs of these two groups differ from those of gun collectors and target shooters. All users, however, appear to have a common interest in technology-enhanced firearms that are as reliable and robust as traditional handguns.

No hard data are available about the amount of money being spent on research and development (R&D) related to smart-handgun technologies.

R&D by the gun industry is probably limited, however. For several years, the federal government has supported a small amount of R&D on smart handguns through a program at the National Institute of Justice. And at least one state, New Jersey, has earmarked funds for smart-handgun research at a state-run university. Taken together, these investments appear to fall well short of the amount necessary to bring a technology to the commercial marketplace in the near future.

Product liability will influence both the ability and the willingness of gun makers to pursue the development of owner-authorized handguns. Guns differ fundamentally from other products in that, in normal use, they are intended to cause harm. Therefore, liability is limited to foreseeable, "unintended" injuries caused by a defect in the firearm. Defects may result from manufacturing flaws, design flaws, or a failure to provide adequate warning of the risks of using the product.

The existence of a defect is based on the state of the art at the time the product was manufactured. The challenge for the courts will be to determine the state of the art at a given point in time. If a technology for owner-authorized handguns matures and is considered state of the art, it is possible that a gun manufacturer could be held liable for *not* incorporating it. In such a climate, the threat of litigation could provide a strong incentive for R&D and innovation. Gun makers who pursue smart-handgun technology might realize a competitive advantage over those who do not. Gun makers who lag behind could risk being shut out of the marketplace.

Given the technical challenges of producing a reliable owner-authorized firearm, however, the fear of litigation could also stifle innovation. Gun makers have three not-mutually-exclusive avenues for addressing the liability threat: creating the best design and warning possible; buying liability insurance; or seeking protection from the government. Legislation now working its way through Congress would prohibit civil liability actions against gun manufacturers for damages resulting from the misuse of their products. The bill provides no protection to gun makers for injuries caused by defective products, however.

Every year, handguns kill and injure thousands of people and are used in the commission of a variety of crimes. Policy makers at the state and national levels, and the public, have focused on police officer gun takeaways and accidental shootings involving children as the problems that can be best addressed by owner-authorized handgun technology. However, these two problems account for a small percentage of the deaths and injuries caused by handguns. According to the FBI, between 1992 and 2001,

46 police officers were killed by service revolvers—either their own or a partner's—in the hands of an adversary (FBI, 2001). Fewer than 200 children under age 20 were killed by unintentional discharges of firearms in 2000, the latest year for which there are data (NCHS, 2002). In contrast, of the 28,663 individuals killed by firearms in 2000, 58 percent (16,586) were suicides, and 38 percent (10,801) were murder victims.

Although most crimes are not committed with guns, the majority of gun crimes are committed with handguns. According to the National Crime Victimization Survey, perpetrators of nearly 90 percent of rapes and sexual assaults, robberies, and aggravated assaults in 1993 used handguns in committing their crimes (Zawitz, 1995). Slightly more than half of the roughly 500,000 guns stolen each year are handguns. A variety of studies have shown that adult and juvenile offenders have stolen firearms or kept, sold, or traded stolen firearms.

Smart-handgun technology could influence the diversion of firearms from authorized to unauthorized users. Diversion occurs through transfers within the home; seizures of handguns from victims by assailants; thefts from homes, vehicles, and commercial locations; and transfers in so-called secondary markets, such as "straw" purchases made on behalf of individuals who cannot legally buy guns. Smart-handgun technology could make unauthorized transfers difficult or unprofitable. Because there are some 70 million "dumb" handguns in circulation in the United States, the impact of technology-enhanced firearms on suicide and homicide rates would depend on their speed of market penetration. The ultimate size of the effect would be influenced by the interplay of a variety of legal, behavioral, economic, and other factors.

The availability of owner-authorized handguns could encourage some people to purchase firearms who otherwise might not, thus increasing the total number of handguns in circulation. The availability of firearms perceived to be "safe" could also have the unintended effect of encouraging people to use less stringent firearms storage practices. And because it might be difficult to tell the difference visually between a technology-enhanced handgun and a dumb handgun, the presence of smart handguns—in the home, for example—could increase the risk of accidental discharges of weapons mistaken for smart handguns.

Given the uncertainties involved and the absence of data, it is impossible at this time to predict whether reliable owner-authorized handguns would have an overall beneficial or detrimental effect, especially in the short term. Despite this uncertainty and the current technical immaturity

of these devices, the potential utility of owner-authorized handguns is intriguing. Considerably more research—in the laboratory and by social scientists—will be necessary to provide manufacturers, policy makers, and the public with enough information to make informed decisions on this important topic.

Workshop Summary

Session 1
Technology for Owner-Authorized Handguns

Speaker Presentations

Dr. Lance Davis, executive officer of the National Academy of Engineering (NAE), opened the Workshop on Owner-Authorized Handguns with some welcoming comments. He explained that NAE's mission is to promote the technological welfare of the nation by marshalling the talents of eminent members of the engineering profession to study issues at the intersection of technology and society, such as the focus of this workshop, owner-authorized handguns. The people attending the workshop, who are involved in the social, legal, or political aspects of gun safety, are well aware that a so-called smart handgun could have an impact on crime and public health and that several technology-related questions are central to the issue. How mature is the technology for owner-authorized weapons? How reliable will these guns be? How long would it take to put them into production? What would it cost?

Dr. Davis noted that the complex issues surrounding smart handguns could not be addressed in a single day and the workshop would probably not provide definitive answers to those questions. The workshop would help NAE frame a future study of the state of research and technology for smart guns.

FIRST KEYNOTE SPEAKER

The first of the two keynote speakers, **Don Sebastian** of the New Jersey Institute of Technology (NJIT), has been involved with the issue of

smart-gun technology for about three years, since the New Jersey Senate began considering legislation to mandate the development of smart-gun technology. (The legislation was enacted in December 2002.) In 2001, NJIT received a $1 million appropriation from the New Jersey legislature to study smart-gun technology in 1999. The legislature appropriated an additional $500,000 in both 2000 and 2002 to supplement the first award.

The legislature mandated that the study focus on smart guns that could address the issue of child safety in the home (legislators used the terms "child-safe" guns, "owner-only" guns, and "smart" guns interchangeably). The legislators wanted to address three concerns: accidental shootings, deliberate crimes by children, and teen suicides. Dr. Sebastian said that NJIT willingly pursued the study under those terms—not for the money but because the institution has always been willing to tackle difficult public-policy questions. Such work, he said, is part of the institution's responsibility as a technological research university.

With the appropriation, the NJIT study focused on three critical questions: Does smart-gun technology exist? If it doesn't but is possible, what would be needed to bring it to the commercial marketplace? Finally, what can NJIT do to bring smart guns closer to market?

One of the first discoveries the NJIT researchers made, Dr. Sebastian said, was that "smart gun" is a term of art. People talked about smart guns as if one existed; there was not an engineering definition of it much less an actual product. The researchers also observed that most people believe that the technologies to create a smart gun already exist. It was, people thought, just a matter of desire for all of the pieces to be put together. The team also learned that a single smart-gun design was not likely to solve all handgun safety problems.

As background for the NJIT study, the team looked into a study (Weiss, 1996) conducted by Sandia National Laboratories in 1995 with funding from the National Institute of Justice (NIJ). That study had focused on the problem of law-enforcement "take-away"—when a police officer's gun is taken away during a crime. The New Jersey legislature, in contrast, was concerned with guns owned by private individuals. Whereas police weapons must be protected from an array of potential abusers, household weapons must be protected most of all from family members. The NJIT researchers concluded that a typical gun owner could not be depended on to adhere to rigorous standards of gun safety. Owners often do not use locking devices or maintain the integrity of the ones they do use. As an example, Dr. Sebastian cited some extant devices that depend on a personal

identification number. The research team found that the codes became common knowledge in a family, and that most codes could be easily discovered by hackers. In short, private gun owners need a technological solution that performs well despite neglect and abuse. Police officers need a technology that will guard against illegal transfer and perform well while the owner maintains strict, rigorous procedures.

Gun hobbyists and sports enthusiasts have entirely different needs, according to Dr. Sebastian. The main concern of these gun users is very likely accidental discharge. Some firms are already working on smart-gun technologies to deal with that issue.

The NJIT researchers developed a list of requirements for home-owner handguns. When not in use, the gun would have to be in a protected mode yet be ready to fire. The gun would have to be able to identify its rightful owner without time-consuming, cross-modal actions.

People often assume that a single technology will solve all of these problems. Popular expectations tend to focus on technology based on fingerprints or voice recognition. Dr. Sebastian emphasized, however, that solving all of these problems will require a systems approach. A gun that turns on when it recognizes a legitimate user will have to be based on a system that integrates several technologies.

During the study, NJIT worked with the New Jersey-based Joint Services of the Small Arms Program (JSSAP), which designs sidearms for the armed services. JSSAP tested 18 commercially available lock-on, bolt-on handgun safety devices and concluded that all of the products manufactured for home use could be compromised with relative ease. In fact, they concluded, none was any better than a traditional lock box.

NIJ is also funding research on electronic analogues of a lock and key. Designed for law enforcement, most of these technologies require a device worn on the person, such as a ring or watch, that communicates with the gun by radio frequency (RF) or ultrasonics. In a home environment, however, the "key" component of these systems is likely to be stored near the gun or in an easily discovered hiding place. And so these technologies, although important from a research standpoint, are not well suited to home use.

To create a true smart gun, according to Dr. Sebastian, it will be necessary to develop a system that uses an attribute of the user or owner—a biometric—as a nontransferable token, a key that cannot be counterfeited or shared. Moreover, of the technologies that might be used in smart guns, biometrics seems to be the most mature. Biometrics are being

investigated for an array of other uses and, therefore, already have a fairly diverse market demand.

NJIT researchers studied commercially available fingerprint identification devices in the laboratory. Although these devices have not been embedded in guns, they are already in common use, typically to provide computer-related security. The team studied four fingerprint-recognition technologies—one that used optical scanning, two that used capacitative measurements, and one that used infrared. The hardware was tested with commercially available software and with a more sophisticated pattern-recognition software developed by BES, a New Jersey company. They also tested BioMouse, an accessory for a computer mouse used in the log-in process in e-commerce to verify purchaser identity. But Biomouse, the size of a traditional optical scanner, cannot be miniaturized to fit inside a gun.

The mechanical failure rate of traditional handguns is around 1 in 20,000. With fingerprint devices failure rates were at best 1 in 100; at times, the failure rate was as high as 1 in 4. The best result with these devices was a 99 percent recognition rate, and that rate could only be achieved under pristine laboratory conditions, with the sensor stringently cleaned between every use. And that rate is about two orders of magnitude higher than the mechanical failure rate. Trying to capture a fingerprint with a fixed sensor, the researchers concluded, would be difficult in real-world situations. In addition, there was no apparent technological growth path for any of the sensor technologies that would bring the failure rate down to the ideal rate. This does not mean that fingerprint technology should be discarded, but it does suggest fingerprint technology might be more effective if it were integrated into a multisensory approach to user identification.

The NJIT team next looked into using the way each person grabs a gun handle to differentiate among gun users. The researchers captured hand placements and sizes from several hundred people to see if they could be used to identify individuals. Hand size was fairly reliable they found, although reproducibility was better for practiced handgun users, such as law-enforcement professionals, than for non-users. When the researchers added sensors to the grip that measured grip pressure during the period of trigger squeeze, the trace of the grip over time could be used to differentiate among hundreds of different users. Satisfactory results were achieved with as few as nine pressure sensors. The NJIT laboratory is now experimenting with micropatterning inside the hand grip of the guns used by the New Jersey State Police.

Dr. Sebastian said he foresees a system approach based on multiple modalities. If one technology has a 1 in 100 failure rate, and another has its own 1 in 100 failure rate, when they are used together, they would have a 1 in 10,000 failure rate. That rate would approach the rate of mechanical failure.

Dr. Sebastian noted that many people think gun manufacturers should be able to develop a reliable smart gun using their own R&D capacity. He estimated that total annual revenues for the gun industry are about $500 million and a reasonable investment in research of 1 percent—or $5 million per year—would not be enough to bring a smart handgun to the marketplace. In fact, he said, neither public entities nor private firms will be able to create smart guns on their own. Gun manufacturers do not have the necessary expertise in software development and microsensor technologies. Public entities simply do not have enough funding to carry out the research on their own. Some sort of public-private partnership will be necessary.

NJIT is now working on a small project with the Picatinny Arsenal to evaluate hand-grip technology in live-fire situations using advanced simulation environments. NJIT has also submitted a proposal to NIJ to create grip-dynamic technology and validate it in live-fire situations. But this is an enormous undertaking, and as the technology gets closer to real-world testing, the costs of development will increase exponentially.

Training a weapon to recognize its authorized user is a real concern. At present, NJIT has developed a grip template that uses 30 "trigger" points to recognize the user—10 points as a baseline and the remaining 20 to establish its robustness. One important question that has arisen is whether a user's profile changes in stressful situations. Handguns in private hands present different problems. If a gun comes with a simple home-use kit—if the process is very open—children might be able to reprogram the gun themselves. Would that invalidate the authorization? Different states already have different policies regarding handgun safety, and states may also demand that they be allowed to train and validate weapons in their own ways.

Dr. Sebastian said there is an acute need for solid, platform-independent, technology-independent standards for legislation regarding smart guns. The standards must be appropriate for the application environment and must specify the levels of recognition and reliability a smart gun would be expected to provide. Only such neutral, objective rules would provide technology developers with standards for judging the suitability of a particular technology or system.

Eventually nontechnology issues, such as product liability, will also have to be addressed. Dr. Sebastian emphasized that even though gun

manufacturers are working on the problem of smart guns, unless the matter of liability is resolved, smart guns will never reach the marketplace. Another important issue is the question of proprietary rights. If smart guns are developed through public-private partnerships, who will produce the new weapons? Who will have the right to distribute them and to train people to use them? When smart guns are ready for sale, who will administer and authenticate the technology?

Moreover, the entire issue of deployment and enforcement could stray into the sensitive area of gun control. These problems will have to be addressed early on, before they become explosive and expensive to address.

SECOND KEYNOTE SPEAKER

John Wirsbinski of Sandia National Laboratories, the next keynote speaker, talked about a very different user group for smart guns: law-enforcement personnel. In 1994, he said, NIJ asked Sandia to take a systems engineering look at the problem of law-enforcement officers being killed in the line of duty when their own weapons were used against them. Sandia's 1996 report was based on that review. More recently, NIJ asked Sandia to take another look at the gun take-away issue to determine how the technology has evolved (Wirsbinski, 2001). Both reports were driven by an assessment of user requirements and focused on systems engineering. The first report used a key analogy: a key, a lock, and a discriminator. In the second report, keys and discriminators were examined from the perspective of access control.

The term smart gun has become such a catchall phrase that the Sandia researchers felt it essential to establish categories to distinguish the types of smart-gun technology. Just as there are several ways to get into a building, there are several possible ways to limit access to a gun. The first way is with mechanical safeties. These are not really smart-gun technologies because they cannot keep a gun from being used by anyone who knows how to operate the mechanical device. However, Mr. Wirsbinski said that he had heard of at least two cases in which a mechanical device on a police officer's gun had delayed an adversary from firing long enough for the officer to regain control of the weapon. Some types of mechanical devices are not very helpful, however. Trigger safeties, for instance, cannot prevent the deliberate firing of the weapon by an unauthorized user—with the safety off, the gun will discharge no matter who pulls the trigger. Mechanical thumb safeties, however, could delay adversaries for a brief period.

Another type of access device is a gun lock. Gun locks are commercially available now, both as retrofits and integrated in new firearms. Many are token based, requiring a key. One problem is that the keys tend to be universal, so anybody could have one. But the mere act of locking a gun does provide some security, although it probably would not be very useful in a law-enforcement scenario. It would be hard to imagine a police officer carrying around a locked weapon, and having to get out a key to use it. Police officers could use gun locks when it was necessary to relinquish a gun, if it had to be stored for a period of time, for instance.

Most current technology development is focused on self-locking weapons that revert to a secured state when they are released from a firing grip. Right now there is a great deal of discussion about technologies to realize such weapons, such as magnetic rings and biometric approaches, including grip scans and fingerprint readers. One company is experimenting with thermal scans of subcutaneous structures. In a law-enforcement scenario, the latter approach could pose problems. For instance, wearing gloves might affect the scan. Another company is producing a fingerprint reader that uses sound waves that can actually penetrate gloves, which might resolve some of the problems associated with fingerprint scans.

The ideal solution for law enforcement is a truly personalized weapon, which will almost certainly be an evolution of a self-locking weapon. But a self-locking weapon, by definition, can only offer a partial solution because it cannot satisfy all of the requirements established in Sandia's 1996 report. But no self-locking weapon is available now; and none will be available in the near future. Producing such a weapon will require systems integration, which is always a troublesome engineering problem. In addition, miniaturization issues will have to be addressed.

Most likely, the solution will emerge from one of two technologies: biometrics or a system using an RF transmitter. One promising type of RF transmitter would be a weapon activated by a chip embedded in the user's hand. Mr. Wirsbinski told the audience that when he first heard this technology proposed as an answer for a self-locking weapon, he did not take the idea seriously. But such chips are already being used in other fields. They are surprisingly popular in health care, for example, where they are used to embed vital medical information that patients always carry with them. Embedded chips have also been used for quite some time to identify purebred animals. Using this technology for a user-authorized weapon would require a small coil inside the gun to generate an induction field with enough power to retrieve information from a chip embedded in the

authorized user's hand. The embedded chip concept would resolve a number of problems with locking technology, such as the possibility of losing a magnetic ring. Mr. Wirsbinski said he has been approached by a gun manufacturer in a country whose military was interested in developing such a weapon for its special forces. In the United States, Mr. Wirsbinski said, developing such a technology for use by police would introduce troublesome privacy issues.

Before biometric user-authorized weapons become common, Mr. Wirsbinski said, many hurdles will have to be overcome, including user acceptance. A few years back, he said, he had worked at an Air Force facility that had just put in place a huge new access-control system that included retinal scans, card swipes, and pin codes. Soon after the system was implemented, a general came through and flatly refused to submit to the retinal scan. He said, "You are not scanning my eyeball with a laser; I don't trust it." The retinal scan was turned off. Another serious issue in the law-enforcement community is reliability. It will be essential that any new technology be proved as reliable in everyday use as the technology the police have now.

Another very complex issue is training handguns to recognize their authorized users. Access control is based on the idea that there is a central location where the access-control database is stored. It is analogous to using a badge reader to get into a building. When you swipe the card, data on the card are compared to data in the computer database, a relatively simple matter. But with a biometric weapon, things would be more complicated. Ideally, the weapon itself would carry the database. When the weapon is in enrollment mode, it would build a template of the authorized user. Then, when it is in use, it could recognize the user, either by comparing his or her template to all of the templates in the database and looking for a match or by directing the system to compare the biometric reading to the specific template of the user to confirm his or her identity. But for a handgun to carry the entire database of stored templates, enormous technical challenges would have to be overcome.

Another potential problem in training a biometric weapon is that a user who is properly enrolled onto a biometric weapon may not be recognized because the template can be thrown off by user stress. When the body goes into fight-or-flight mode, many things change, such as blood flow, muscle tension, and even physical structures. At these times, things that were learned in an unstressed situation become inaccessible. How can biometric gun technology cope with this reality?

Another problem with biometric weapons is false rejections. Over the years, researchers have learned that for the first two to six weeks after biometric and access control devices are deployed, they have a higher false rejection rate. Once the user is well trained, the devices work far more reliably. Whether this will happen with firearms is an open question. In addition, when a biometric device is not used for an extended period of time—six months, perhaps—the false rejection rate recurs. The biometrics community is not sure whether this is a function of an aging template—that a person's biometrics change over time—or whether it is a function of user training. In either case, this could be a serious problem. Many officers leave their guns holstered for extended periods of time, and many never fire their weapons at all in the line of duty.

The two biggest changes in smart-gun technology since the Sandia group's 1996 report have been evolutionary rather than revolutionary. First, there is now a commercialized electronic primer technology, which is used only in long arms. Second, some manufacturers are looking into totally electronic weapons. In fact, a few prototype "proofs of concept" have been created. In these guns, the bullets are stacked in the barrel, and the priming compound is stacked in the barrel; there are no mechanical operations. No self-contained cartridge is chambered and ejected. Everything is electronic. But, this also raises some serious issues. Mr. Wirsbinski asked the audience to think of how personal computers work and decide if they would be willing to bet their lives on the reliability of electronics. In addition, electronic guns would require the development of a totally new manual of arms.

These technologies may one day lead to the development of a smart gun. Many of them are promising and some of them suggest answers that might work in certain situations. But, so far, none of them meets the needs of law enforcement.

Panel Presentations

The panel session opened with remarks by **Ken Green,** who represented the National Shooting and Sports Foundation and the Sporting Arms and Ammunition Manufacturers Institute (SAAMI). Established in the early 1900s, SAAMI's purpose is to set standards for the manufacture of firearms and ammunition.

Currently, SAAMI has 25 member organizations, but the standards apply to all commercial manufacturers of firearms and ammunition. SAAMI has set some 700 standards, covering the dimensions of cartridges and chambers, the velocity of projectiles, and chamber pressure for rimfire pistol, revolver, shotgun, and rifle cartridges. There is also a standard for the abuse and mishandling of weapons. Many of the standards are listed with the American National Standards Institute (ANSI), and all are voluntary, although most manufacturers do follow them. ANSI standards documents may be seen on its website, ansi.org. When the technologies for user-authorized guns become available, standards will be set for them as well.

Kevin Foley, a representative of Smith & Wesson, said that his company has been working in the area of user-authorized weapons for some time. The company acted in an advisory capacity during the 1996 study by Sandia National Laboratory (Weiss, 1996). Once the study was completed, he said, Smith & Wesson became more active in researching the technology. All of Smith & Wesson's revolvers are now sold with integrated mechanical locking systems. By next year, the locking systems will also be on

all of its pistols, thus meeting the legal requirements for several states. The company has provided external gun locks since 1997.

Smith & Wesson has experimented with placing electronics and other devices inside a conventionally produced handgun. The handgun would then fire only when a user wore a wristwatch-type transponder. One problem with this approach involves the mechanics of a gun. The inside of a conventional handgun is entirely mechanical, with levers, springs, and pins. To prevent the trigger from firing, the linkage between the trigger and the firing pin must be disconnected or blocked. This might be done by adding a separate, microelectromechanical system (MEMS). But the Smith & Wesson researchers found it would be impossible to make the MEMS reliable. Because handguns are designed to be field stripped, disassembled, and cleaned, a MEMS device could be easily disabled. Besides, it would be very easy to bypass a sophisticated electronic security system inside a handgun.

Transponders, which are essentially electronic keys, also turned out to be unsatisfactory. When Smith & Wesson researchers compared transponders with the key locks the weapons industry had been providing for some time, they concluded that transponders offered no additional benefit. In the officer take-away situation, nothing was gained.

Based on these experiences, Mr. Foley said, the research team set some design goals. First, the reliability and durability of the weapon must not be compromised by a security system. Second, if the security system is removed, the gun must stop functioning and become useless. Third, there should be no keys. An authorized-user-only weapon should function, or not, based on the user's identity, not on what the user brings to the gun, he said.

The Smith & Wesson team concluded that the design goals could only be met by eliminating the mechanical firing mechanism and designing the weapon so the electronic security system could be integrated into the firing mechanism. The user would be identified by biometric information, and identification could be instantaneous. If the authorized user picks up the gun, it will function, but if anyone else picks it up, it will not.

At this point, the research team examined Remington's EtronX primer, which is used in rifles that fire cartridges electronically. A rifle stock has a lot more room than the handgun grip. Beginning in 1997, Smith & Wesson has worked to miniaturize the technology for electronic firing. At this point, company researchers have fired about 50,000 rounds of ammunition and are building 50 handguns, a number of which have fired more than 5,000 rounds. But the space is very cramped inside those guns, and they are not

perfect. Mr. Foley said that attaining a durable and reliable system is becoming increasingly feasible.

Working with funding from the National Institute of Justice (NIJ), Smith & Wesson's next step will be to miniaturize the firing electronics to make room for biometrics. The company is working with a biometrics company in New Mexico to develop a small light emitting diode (LED) sensor that conforms to the grip but that does not rely on fingerprint image, so that grip placement does not have to be precise. The electronics are small and fast, and the performance of the gun has the potential to be as good as or better than anything else the researchers have seen.

The team is now past the proof-of-concept stage. In March 2002, the company built its first solid-state system, which is now being tested. Mr. Foley said Smith & Wesson researchers are about two years away from a handgun with integrated biometrics that can be tested in the field.

The next speaker, **Peter Sebelius** of the Charles Stark Draper Laboratory, noted that since September 11, 2001, research on biometric identification has increased dramatically. Identification by biometrics, he said, is an interesting process, one that has tended to focus on the automation of mechanical systems already in use. Mr. Sebelius argued that biometric identification should take a more expansive approach. Just as people identify each other by drawing on several senses, similarly, biometric identification should use multiple sensors and an automated judgment, or weighting, scheme.

Examples of judgment schemes are already in use. Fault-tolerant systems, for example, draw input from multiple sensors, sometimes sensing the same things and sometimes sensing different things. This kind of system is used in the SSN-21 submarine, where four flight-control-system channels measure the vessel's position and movement, then instantaneously "vote" whether the computer has come to the right conclusion as a result of the sensor input. If one channel or component fails, the other channels recognize that, shut the system off, and then continue to operate in a reduced mode, while issuing warnings about the failure.

Training is vital to using the system, and it will be vital that handgun users be trained to use biometric weapons. Although, as one participant in the conference pointed out, federal law does not set requirements for handgun ownership, many states require that owners be trained to use handguns. At that time, owners could also be trained to use biometric identification features.

It is also important to remember that mechanical safety devices are already available commercially but are often not used. Often in the gun-related tragedies reported in the media, for instance when a child takes his father's gun and shoots a classmate, all of the extant mechanical locks were available to the father. A trigger lock could have been put on the gun or the gun could have been put in a cabinet and the key kept by the father. Mr. Sebelius recalled one workshop participant pointing out that a national survey of private firearms ownership indicated that of households with handguns only 43 percent kept them locked and unloaded (Cook and Ludwig, 1996). Even fewer households kept guns unloaded.

Another issue that arises in this context is the reliability of an electronic device. Mr. Sebelius argued that we already trust many electronic devices. We trust electronic watches to tell time. When we fly, we trust computers with our lives. A lot of work is being done to create trustworthy electronic weapons.

Naeem Zafar of Viridicom, a spinoff of Bell Labs located in Silicon Valley, noted that his company is working on fingerprint-sensor technology and fingerprint-sensing algorithms. The company has commercialized a silicon sensor and holds some of the original patents on the technology. Three patent applications related to these technologies are in different stages of the patenting process. He said Veridicom's sensor is the most widely used fingerprint sensor in the world.

The biggest market for biometrics, he said, is in South Africa, where government payments are made on the basis of fingerprint identification. The same technology is becoming popular in China, where the government has issued national identity cards to every citizen in the form of smart cards carrying two fingerprint sensors. The technology is also being adopted in Malaysia, Hong Kong, and Italy, he said.

Eventually, it will be possible to put biometrics into the gun itself, but many questions will have to be answered first. Biometrics-based handguns will not be accepted unless they are safe and simple to operate. It is fine to investigate exotic technologies, but, ultimately, the police want a gun that is deployable and does not hinder critical actions. Sometimes, he said, police must just pick up a gun and shoot, with no time to think about placing their fingers just so.

At Veridicom, researchers are approaching the take-away problem not as a matter of securing a gun, but as a matter of securing gun access. One solution Veridicom is now pursuing is a secure holster. The holster looks

like a normal holster and can carry a normal gun, but it has a fingerprint sensor inside that unlocks the gun once it confirms the print. Recognition takes only a few milliseconds. The holster, he said, is convenient, simple to program and use, and keeps a record of the last 500 people who tried to access the gun. Right now, as a specialty item, the holster costs around $100. When it enters mass production, the cost will drop to about $20.

Mr. Zafar's associate, Andrew Eros, president of AcciMetrix, the company working with Veridicom to assemble the holster technology, said that if the device does not recognize the user, the gun remains locked in the holster. The holster is powered by a 9-volt battery and has a shelf life of one year. When the battery fails, the holster releases the gun. If a catastrophic failure should occur, for instance if the gun is dropped and accidentally discharges, the holster keeps the gun locked in place. Mr. Eros said that the holster, which he described as an intermediate solution to the problem of gun take-aways, will enter production when testing is complete, perhaps by the end of 2002.

In reply to a query about whether fingerprints are unique enough identifiers, Mr. Zafar said fingerprints are more individual than many other identifiers now in common use, such as PIN numbers and passwords.

Veridicom has been working on ways to circumvent certain fingerprint-sensor problems. For instance, currently the technology will not work when a user is wearing gloves or when fingerprints are coated with various solvents and household products. The company has recently introduced software that can screen out "old" (latent) fingerprint impressions on the sensor in order to read only the current print.

In reply to a question about fingerprint registration as being tantamount to handgun registration, Mr. Zafar said that the fingerprints represent the gun owner's relationship to the gun. They are not currently registered with the government and do not pass into a centralized database but remain in localized databases on the weapons themselves.

In the last three years, the reliability of fingerprint-identification technology has improved enormously. Veridicom's testing with the 1.2 million registered users in the South Africa database has reduced the failure rate to 1 in 100,000.

Fingerprint-recognition technology is being deployed more widely than in just weapons applications. For instance, it is finding many uses in securing medical records. And as part of an access-control device, Veridicom's chip is built into PCs made by NEC, Fujitsu, Acer, Panasonic, and Hitachi; its competitor's chip is built into Samsung and Micron equipment. About

45,000 PCs a month are sold with the Veridicom chip built in. Mr. Zafar said he believes everyone will eventually have some kind of small biometric device, on a keychain, perhaps, or an electronic ring, for everyday consumer transactions—to pay for groceries, open a car door, log onto a PC, or protect valuable digital content, such as music.

Wendy Howe, a program manager in the NIJ Office of Science and Technology, defined the purpose of NIJ, the research arm of the U.S. Department of Justice, as improving the criminal justice system, either through the identification and modeling of programs in the social sciences, or through improvements in science and technology. The Office of Science and Technology began supporting research on smart guns in 1994, prompted by the gun take-away problem in law enforcement.

Police officers have very specific views about what they need in a smart gun. They do not want weapons that require wearing a secondary unit, such as rings on both hands or watches on both wrists or badges or pagers that carry the technology. The recognition technology and power source needed to be transparent and seamless. They don't want to go through extensive training, and they want new weapons to resemble the weapons they already know.

The 1996 Sandia report found that one of the most critical feature to law-enforcement officers was that, if the power source in the smart weapon failed, the weapon would revert to a normal sidearm; in other words, it must "fail live." Thus, the officer could still use the weapon, but in the event of a take-away, so could the assailant.

Another important concern is related to multiple authorized users. Most law-enforcement agencies in the United States have fewer than 25 officers. Sometimes, an entire department must have access to one weapon; in certain situations, partners must share a single firearm. Particular units, such as SWAT teams, often share weapons.

Everyone wanted the weapon to be cost effective, preferably a technology that could be retrofitted to existing guns so that police departments would not have to strain their limited budgets to buy new weapons.

In addition to the report, Sandia produced several proof-of-principle devices—actually boxes containing air pistols and electronics and a power source. Ms. Howe's team then attended conferences of major law-enforcement organizations, such as the International Association of Chiefs of Police, the National Sheriffs Association, and the Fraternal Order of Police, as well as technology fairs in local communities. At each venue, they

demonstrated the devices and described the research process, addressing technology issues, such as voice recognition and magnetic rings.

The boxes were a difficult sell because they were rudimentary and could not demonstrate the full potential of the recognition technology. But these demonstrations did provide opportunities for law-enforcement personnel to discuss their requirements for such a firearm. For instance, some officers pointed out a serious flaw for police in voice-recognition technology—an officer could not "talk to" his or her gun without revealing his or her the location to the suspect. The higher up the chain of command, the greater the interest in the proof-of-principle devices. Command staff was far more interested in the liability issue associated with smart guns than line officers, who typically saw only a cumbersome box containing an air pistol. When the NIJ team exhibited a 40-caliber weapon (developed by Colt) that authorizes the user through a radio-frequency technology contained in a wristwatch, many officers were very receptive because the gun was similar to the ones they already use and was activated by the mere presence of a watch.

In 1999, in response to a public solicitation for proposals, NIJ awarded nominal grants ($300,000 each) to Smith & Wesson and to FN Manufacturing for smart-gun technology development. In 2000, after Congress appropriated $8 million in new money specifically for smart-gun research, NIJ provided significant funding to Smith & Wesson for its electronically fired, biometric recognition firearm, and FN Manufacturing's ultrasonic with embedded microelectrnics identification weapon. NIJ also funded Sandia to update the 1996 study, and it released a directed solicitation for the development of smart-gun technology.

NIJ's goal was not to have one universal smart-gun technology for all firearms but to provide seed money to bring several promising technologies to fruition. Of the 12 proposals that were submitted for independent peer review, Ms. Howe said four were funded. The proposals used various approaches, including additional biometric recognition systems, chemical compounds and radio-frequency technologies. Two of the four projects—one using ultrasonic technology together with a transponder, and one using biometric identification in an electronically fired weapon—are moving forward very well and have gone through independent peer reviews with law-enforcement agencies to determine the functionality of the firearms in controlled operational settings. The grantees include VLe Small Arms, Exponent Inc., Technology Next, and Mosermation.

Ms. Howe said that it will be at least five years before there is a weapon capable of undergoing rigorous laboratory and field testing. A smart gun for law enforcement will not be ready for many years.

Session 2
Liability Concerns

Speaker Presentations

Under product liability theory, a gun manufacturer is not at legal risk simply because it produces a dangerous product, said **Prof. David Fischer,** keynote speaker at the second session. Prof. Fischer is the James Lewis Parks Professor of Law at the University of Missouri, Columbia, and the author of *Products Liability: Cases and Materials* (West Group, 2002), a leading book on torts cases, as well as numerous scholarly articles on tort and product liability law. The key determinant of liability, he said, is that the gun be defective. For a manufacturer to be liable, the gun has to malfunction in some way.

A product liability action must meet several conditions, Prof. Fischer explained. First, the defendant must be in the market chain of distribution (e.g., a manufacturer, wholesaler, retailer). A casual seller would not be subject to product liability. Second, the gun must be defective, and the defect must emerge while the gun is used as intended. There is no requirement that a product protect against an unforeseeable misuse. Product liability applies to physical harm to persons or property, not to pure economic loss.

There are three kinds of defects: manufacturing flaws, design defects, and warning defects.

MANUFACTURING DEFECTS

Manufacturing defects are quality control failures. Ten thousand tires come off an assembly line; because quality control measures failed, one has

a flaw and blows out. Because the product deviates from its intended design, the manufacturer is liable for physical harm caused by the flaw. Manufacturing defects are relatively rare, and such cases constitute a small percentage of product liability litigation.

DESIGN DEFECTS

Design defects account for a much larger percentage of liability litigation. These cases are based on allegations that the design makes the product excessively dangerous. If a plaintiff succeeds in persuading the court of this, it could have serious implications, because every product off the assembly line has the same defect.

Product liability law is a common-law system. Each state has its own product liability law; the rules are remarkably similar, but there are some significant differences. To escape liability, however, manufacturers must live up to the standard of the most stringent state law. Moreover, to determine whether a product is defective in design, the most common risk-utility test balances (1) the risk associated with using the product against (2) the burden of taking steps to eliminate the risk. With firearms, the consequences of a design-related mishap can be quite serious. Not all jurisdictions require proof of a safer alternative design, although plaintiffs often come into court and present evidence of a safer design to the jury.

Some jurisdictions use a consumer-expectations test. Even if there is no liability to an open and obvious danger, the product is defective if it contains an unknown, unexpected danger. In these jurisdictions, the question is whether the danger is known. Would a handgun that doesn't have owner-authorized technology be defective under this test? Probably not, because today people do not expect guns to recognize owners. But if in the future people do expect that, under this test a gun could be considered defective.

Most jurisdictions, however, use the risk-utility test. The burden of protecting against risk involves many factors, such as the feasibility of implementing a safer alternative design. The court must decide if it is mechanically, physically possible to implement the safer alternative today. This means manufacturers are held to the standards of experts; they are required to keep up with the state of the art. The risk-utility test, however, also requires taking into account the cost of the safer alternative design. In this case, cost is not just the expense of the alternative design, but also the adverse consequences to the user and the usefulness of the product. For instance, it would be possible to put a governor on an auto engine that

would make it impossible to drive faster than 20 mph, which would dramatically reduce the number of road accidents and injuries. But this would also interfere, to a degree unacceptable to users, with the usefulness of the product. So no one requires that. A plaintiff must persuade a jury that a manufacturer could have adopted a safer alternative design that would have eliminated the risk in question, taking into account the cost of the device and the possible impairment to the product's functioning resulting from the new design.

Hammond v. Colt Industries, a 1989 Delaware case, involved a replica of a nineteenth-century Colt revolver loaded in all six cylinders. A 13-year-old twirled the gun around his finger and the gun shot him in the head. An action was brought on his behalf charging that Colt should not have sold a gun with a primitive nineteenth-century safety device that did not work. Plaintiffs argued that Colt should have included a modern safety device to prevent such an accident. The modern safety would have prevented the accident, would not have interfered with the gun's use, and would have been very inexpensive. But a gun with such a device would not have been 100 percent authentic. The jury found in Colt's favor. It decided that in the nineteenth century, when the original gun was made, the primitive safety device was state of the art and that products must be judged according to the state of the art prevailing at the time of original manufacture.

As a corollary to this decision, manufacturers have no duty to recall and retrofit products that were not defective at the time of manufacture. The duty to recall only applies to defective products, Prof. Fischer said. Recall is required when mandated by a government agency, though many companies recall defective products to prevent injuries even in the absence of a mandate.

One of the challenges facing a manufacturer of a user-authorized handgun is determining the state of the art at the time of manufacture. Assume, for example, such a firearm goes on the market in 2010. By 2012, the technology will already have evolved rapidly. If in 2020 a lawsuit is brought against a manufacturer for failures in that 2010 gun, one of the things litigated would be whether the gun's makers complied with the state of the art of 2010. Could they have done better?

A workshop participant posed this hypothetical situation: In the year 2010, a gun manufacturer makes 21 gun models. Twenty are conventional weapons, but the twenty-first is a "smart" gun. If that gun proves successful, could it be argued that the 20 other models are defective, that the manufacturer could have made them better? Prof. Fischer replied that if

alternative products are offered, and neither is defective, then there is no liability. An analogy might be cars, which come with and without antilock brakes. However, if smart-gun technology becomes very good, as it might by 2020, then the legal issues could change. Someone selling a conventional gun after that date could be liable for selling a defective model because the expectation would be that all new handguns have technology that recognizes the authorized user. In this scenario, manufacturers with smart-gun technology, or simply the patents on the technology, would have a huge competitive advantage.

It is not enough for a plaintiff to come up with just any alternative design, Prof. Fischer explained. The new design has to be better overall than the design that was used. A simple example is the use of shatterproof glass in the side windows of automobiles. Putting shatterproof glass in the side windows would completely eliminate the risk of injury by flying glass in an accident. But in a different kind of accident, if the occupant is trapped inside the car, the shatterproof glass would prevent rescuers from reaching the occupant of the vehicle. So putting shatterproof glass in side windows eliminates the risk of one kind of injury but increases the risk of a different, and more catastrophic, injury. In the risk-utility model, these risks must be balanced. A manufacturer may have to make hard choices, and a plaintiff can always argue that the choices were wrong.

User-authorized handgun technology can present this very problem. For example, if a manufacturer chooses to use a radio transmitter inside a ring, the gun owner might be able to fire the weapon with only one hand. What happens if that hand is injured? If the range of the sensing device is increased, then a criminal could take the gun away and shoot the owner. By solving one problem, you would create another. Fingerprint technology also has problems, as was discussed earlier. No technology is perfect, and every technology could end up being criticized under one theory or another. That is the dilemma gun manufacturers face.

Typically, Prof. Fischer said, a product is proved defective by inspection by an expert. But sometimes products are not available for inspection, if they have been destroyed or stolen, for instance. Is there any way to prove that a gun is defective if the gun is missing? Some cases suggest that, under certain circumstances, if a product fails to perform its manifestly intended function, the failure can be inferred to be the result of a defect.

If, for example, the steering in a new car fails without warning, and the car hits a tree, one can probably infer that this happened because of a defect

and that the car was defective when it left the manufacturer. But if the car is three years old, the situation may be different. The steering failure may have resulted from a defect, but there is no reason to believe that the car was defective at the time it left the hands of the manufacturer. The defect might have been introduced at a later time.

How does this apply to owner-authorized technology? Suppose a gun allows only the owner to fire it. There could be a failure (1) if it doesn't fire when the owner wants it to or (2) if it fires when an unauthorized person uses it. Is the product defective merely because it failed to work the way it was expected to work? That question can only be addressed by looking at the nature of the technology. But if it is a relatively new handgun that has not been abused or manipulated, we might infer that it was defective at the time it left the manufacturer.

WARNING DEFECTS

The final theory of product liability is the warning theory, which essentially requires reasonable care on the part of the manufacturer. A good warning has three components. First, it must adequately catch the user's attention. Second, it has to adequately apprise the user of the nature of the danger. And third, it has to adequately instruct the user in how to avoid the danger. With user-authorized handgun technology, what would be an appropriate warning? Should warnings be written out in a booklet or inscribed on the gun? The problem with warnings is similar to the problem with designs. There is no perfect warning. A warning that is too detailed, for instance, could be self-defeating itself because no one would read it.

Another problem manufacturers must face is that user-authorized technology will probably never be completely foolproof. There are many ways the technology could fail. Because any choice the manufacturer makes might be criticized, there are also many ways a plaintiff could obtain a legal determination regarding the product's defectiveness. If the product is really good and the manufacturer has done its best to design and to warn, the manufacturer might win the case, but the costs of defending the case could be significant.

A manufacturer could do several things to insulate itself from these potential problems, Prof. Fischer said. It could develop the best technology possible, give the best warnings, and buy liability insurance—and then build the cost of the insurance into the price of the gun. Liability insurance

might enable a manufacturer to bear some of the financial risks associated with selling user-authorized technology—assuming, of course, that liability costs don't drive the price of the gun so high that it becomes unaffordable.

Manufacturers could also seek protection from the government. If the government were to mandate owner-authorized safety devices, it might also implement a scheme to shield manufacturers from civil liability. Manufacturers would favor this, but it might be hard to achieve politically. If liability risks to manufacturers must be reduced through insurance, gun users will finance the system. If government steps in, taxpayers will finance it. These are important policy options about which people disagree.

Panel Presentations

Larry Keane, vice president and general counsel for the National Shooting Sports Foundation, the firearms industry's major trade association, and general counsel to the Sporting Arms and Ammunition Manufacturers Institute (SAAMI), affirmed that the firearms industry is not opposed to the development of so-called smart-gun technology. Many interest groups now involved in litigation, including municipal litigation, say that the firearms industry has suppressed the development and implementation of smart-gun technology, but that is not the case, Mr. Keane said. The participation of representatives of firearms manufacturers in the NAE workshop, and the descriptions of their companies' work in this area, is evidence of that.

The firearms industry's primary concerns about product liability are related to proposed state laws that would mandate the implementation of smart-gun technology. It is abundantly clear from the workshop discussions, Mr. Keane said, that the technology to make user-authorized, or smart, guns is immature. Manufacturers are right to be seriously worried about product liability exposure if they are asked to market products that are not currently reliable and that pose a risk to users and to the general public.

Laws that require the incorporation of unreliable technology in handguns, Mr. Keane said, are bad public policy because they expose manufacturers to unjustified and unwarranted liability. Citing Dr. Fischer's discussion of the contentious issue of immunity from product-liability lawsuits, Mr. Keane said he is not aware of any state legislation that requires the

production of "smart" guns and also provides immunity to manufacturers or anyone in the firearms distribution chain. Mr. Keane noted that there is a bill before Congress intended to prevent what he called "frivolous" lawsuits brought by the Brady Center and other groups against the firearms industry for the criminal misuse of handguns.[4]

A number of firearms manufacturers sell products that incorporate built-in, or internal, locking devices. External locks, Mr. Keane noted, have been distributed for years—for decades by some manufacturers. Although the number of firearms in the U.S. has been rising, the number of accidental fatalities and criminal homicides involving firearms has been dropping, he said. Firearms accidents are at their lowest rate since record keeping began in 1903. These are indications, Mr. Keane said, that contrary to what other speakers had suggested, consumers are using external gun locks. An internal locking device, like an external one, requires that the consumer lock it and unlock it. If, for the sake of argument, one assumes that external locks are available but are not being used, then the same problem of disuse would apply with internal locking mechanisms.

One important question is what constitutes a defect in smart-gun technology. Regardless of the technology, there are significant reliability issues, for instance, issues related to a product's failure mode. Does the product fail so it can still be used, or does it fail so it cannot be used? If one can envision bad outcomes in either scenario, is the product defective?

Consumers ought to have a choice, and manufacturers should have the opportunity to market products that consumers want, Mr. Keane said. A properly functioning firearm is not defective in and of itself; it is designed to fire a bullet when the trigger is pulled. The absence, or presence, of a "smart" device, even if the technology were feasible, would not render the product defective, according to liability principles. The analogy to antilock brakes is a sound one. Another applicable analogy also involves cars. It is foreseeable to General Motors that people will buy cars, that they will drive the cars, that their children will ride in the cars, that accidents will occur, and that some children will be injured. No one would suggest that the absence of a built-in child car seat renders an automobile defective. But

[4]The House passed the bill, Protection of Lawful Commerce in Arms Act (HR 1036), on April 9, 2003. It has 52 cosponsors in the Senate. The legislation would not provide immunity from liability for harm caused by defective products.

there are car models available today with such built-in seats. The absence of a car seat does not make a car defective.

Arthur Bryant, the executive director of Trial Lawyers for Public Justice (TLPJ), a national public interest law firm, said TLPJ has never been involved in gun litigation or taken a position on any gun-related issues. TLPJ is neither pro-gun nor anti-gun.

Mr. Bryant said the law does not require products to be smart, and it does not require smart guns. The law does require that manufacturers act like they are smart and, when a product could injure someone, act like they care. The law generally says the manufacturer has a duty to prevent foreseeable injuries. "Foreseeable" is a mushy term. When that principle is applied to guns, all of a sudden the discussion gets weird, because guns are intended to cause injuries. So with guns, said Mr. Bryant, the manufacturer has the duty to prevent foreseeable unintended injuries.

Manufacturers cannot be expected to prevent all unintended injuries. For example, auto manufacturers can't prevent everyone from being injured in car crashes. Gun manufacturers, no matter what they do, can not prevent all unintentional injuries caused by guns. But the law says that manufacturers have to act responsibly, not negligently; they have to act reasonably; they have to act with the knowledge of an expert. The law says manufacturers are expected to act as if they know more than consumers, because whether they do or not, they ought to.

To act responsibly when making a product, manufacturers must first warn and educate consumers about risks consumers may not fully appreciate. Second, companies must design their products so all reasonable steps have been taken to prevent, in this case, unintended foreseeable injuries. If a new design introduces other problems, the manufacturer should try to modify the design to bypass those problems. Third, manufacturers must do everything they reasonably can to make their products to specifications.

Mr. Bryant said that most workshop participants seem to accept that gun manufacturers cannot reasonably be expected to produce a reliable smart gun at this time. But, he said, many seem to believe that manufacturers could be doing things now that are "smarter" than what they are actually doing. Some of the common-sense, doable things that appear to be superior to external locks are combination locks, transponder rings, and internal locks. But these devices are not being advocated very heavily in the marketplace. In other words, they are not being incorporated into most guns.

Mr. Bryant said there was a dramatic difference, historically, between the attitudes of firearms manufacturers and the attitudes of most other manufacturers toward the duty to prevent unintended injuries. In most industries, products are routinely designed to avoid causing unintended injuries. But the firearms industry has not consistently made design improvements a priority. It appears that the incentives for producing a safer product are not as developed in firearms manufacturing as they should be, and this has contributed to a responsibility lag, Mr. Bryant asserted.

It is only a matter of time, he said, before a manufacturer is held liable for not incorporating, for instance, internal locks or ring technology. When that happens, there will be powerful incentives for other manufacturers to start incorporating the technology.

Mr. Bryant noted that in the early 1980s, the federal government was pushing car manufacturers to install air bags, although the technology was not quite ready. Meanwhile, most cars in America had no rear-seat shoulder belts. The belts cost almost nothing, and they would have prevented some injuries—not a massive number, because most car injuries happen in the front seat. But the federal government waited and waited to mandate them. Around this time, a lawsuit was brought against Ford involving a child who was riding in the back seat wearing his lap belt. The car was in a frontal collision, he jackknifed over, his head hit the front seat, and he ended up with brain damage. In court, the plaintiff's lawyers showed how little it would have cost to install a rear shoulder harness. The case was helped because Ford was already selling cars with rear shoulder harnesses in Europe. There was a multimillion dollar verdict, and within two months, the federal government required that car manufacturers install the harnesses. It was the litigation that drove the change. Don't be surprised, Mr. Bryant said, if litigation over existing technologies—not smart guns, which may be way off in the future—leads to similar quick changes in the gun industry.

The threat of liability can affect innovation, Mr. Bryant said. A study (Huber and Litan, 1991) by the Brookings Institution on this topic found two countervailing forces. On the one hand, the threat of liability encourages innovation. Manufacturers want their products to be safer to avoid lawsuits. On the other hand, the threat of liability can deter innovation because manufacturers may not want to be the first to introduce a new design that hasn't been proven safe. In other words, the threat of litigation encourages manufacturers to introduce safety-related technologies, but it also encourages them to make sure the innovations work.

It is important to remember, he said, that the perfect can be the enemy of the reasonable, the possible, and the good. If it is reasonable and possible to make guns marginally safer now, while also pursuing the long-term goal of a smart gun, then we ought to be acting through policy, litigation, and engineering to implement the steps that could make some difference.

Dennis Henigan, director of the Legal Action Project of the Brady Center to Prevent Gun Violence, said the tort liability system plays an essential role in bringing about design changes intended to prevent the misuse of guns by children and other unauthorized users.

History teaches two lessons about product safety, he said. First, the safety of dangerous products is too important to be left in the hands of the manufacturers of those products. Second, making products safer is not simply a matter of science and engineering. It is also a matter of will—the will to make products safer. Improvements in product safety in any industry depend on how much the industry is willing to invest in research and development. That, in turn, depends on the incentives industry has to make its products safer.

History also suggests that the free market often does not provide a sufficient incentive. The costs of unsafe products generally are not borne by the industries that manufacture them, Mr. Henigan said. Rather, they are borne by the victims of those unsafe products and by the public, through the cost-spreading mechanisms of private and government insurance. In the case of gun-related injury and death, the victims are often not the consumers of the products, nor even related to those consumers. When it comes to guns, the question is not a matter of what consumers ultimately want. Everyone has an interest in gun safety. The reason there has not been greater progress toward product safety in the gun industry is not because the industry lacks resources. Rather, he suggested, it is because the industry has not taken seriously its obligation to prevent misuse by unauthorized persons.

Mr. Henigan asked why more progress in developing smart guns has not been made. The concept of personalization and resistance to unauthorized use has been around for a long time. According to Mr. Henigan, the gun industry has invested in research on ways to pack more firepower into smaller, more concealable spaces. But it does not invest in research and development in product safety.

Developing safer products is a process. Some early innovations may be imperfect, but they are improvements. Why has this process begun for

guns only in the last few years? For most products, government safety regulation and the product liability tort system work in tandem to provide strong incentives to make products safer. For example, the auto industry did not introduce seat belts or air bags or make cars more crashworthy out of the goodness of its heart. It did so because of regulatory mandates and civil liability concerns. Automakers made precisely the same arguments that gun manufacturers use today when talking about making guns resistant to unauthorized use. Auto accidents, they said, are caused not by unsafe cars, but by unsafe drivers; improvements in auto safety will make cars unaffordable, will make drivers more careless, and will ultimately cost more lives than they will save. All of those arguments, Mr. Henigan asserted, were ultimately discarded, and we now expect automobiles to have these safety features.

Mr. Henigan cited another example, cigarette lighters used by children to start fires that endanger not only the children themselves, but sometimes whole neighborhoods. The problem is very similar to the problem of gun owners leaving their weapons where they are accessible to kids. Courts are now beginning to hold manufacturers of cigarette lighters liable for failing to use existing childproofing systems. Interestingly, the manufacturers' defense in those lawsuits has been that the lighters are intended for use by adults, not children. The courts have rejected this defense, holding that the cigarette lighter manufacturers have a responsibility to design lighters that are resistant to use by unintended users. The courts have imposed liability even though the lighters did not malfunction in any way. In *Perkins v. Wilkinson Sword*, the Ohio Supreme Court ruled that a lighter manufacturer may be liable for failing to use a feasible alternative design that would have prevented harm caused by an unintended, but reasonably foreseeable, use of its product.

The Consumer Product Safety Commission (CPSC) now requires that lighters be made childproof. In contrast, guns are specifically exempt from regulation under the CPSC. This is an example of the triumph of raw political power over rationality in public policy, said Mr. Henigan. Guns are the only widely available consumer product that is designed to kill. But there is no federal agency with the authority to recall defective guns or set safety standards for guns. The gun lobby has succeeded in winning the industry that exemption. That means the only incentive to get the gun industry to take its safety responsibilities seriously is the threat of damages liability. Now the industry is trying to immunize itself from the civil liability system as well.

The firearms industry is desperate for immunity from liability when a tragedy results from an unintended use of a gun. This is because the courts are now starting to find gun manufacturers liable based on an argument similar to the one affecting manufacturers of cigarette lighters. In a case brought in New Mexico last year, *Smith v. Bryco Arms*, the New Mexico Court of Appeals issued a landmark ruling holding that a gunmaker could be held liable for failing to install safety mechanisms in guns to prevent unintentional shootings by minors. The safety mechanisms at issue were a magazine-disconnect safety and a load indicator, not an integral locking device. Significantly, this ruling was handed down in New Mexico, in gun country. The court said the manufacturer of a product intended to be lethal has a greater responsibility to make it less accessible to foreseeable but unintended users.

The gun industry has great reason to be concerned about its potential liability for failing to move forward on product safety, Mr. Henigan asserted. Allegations based on the industry's failure to make guns more resistant to unauthorized use are a part of most of the municipal lawsuits his group has filed against the gun industry, he noted. Most of those cases have survived motions to dismiss.

The substantial threat of liability is having a profound impact on the industry's behavior and on the design of guns. Prior to 1995, when the Brady Center filed *Dix v. Beretta*, the first lawsuit focused on a manufacturer's failure to install a gun-locking mechanism, not a single U.S. gun manufacturer had made or sold a gun with an integral locking system. Now, there are at least seven. Mr. Henigan said he doubts the change reflects legislative mandates, because only one state, Maryland, has passed legislation that requires new handguns to have an internal locking device.

Mr. Henigan said that the gun industry's contention that gun owners are hostile to personalized technology is false. A study in the *New England Journal of Medicine* three years ago (Teret et al., 1998) found that 59 percent of gun owners favored legislation requiring all new handguns to be personalized.

Many groups are opposed to the concept of owner-authorized guns, but there is simply a compelling logic to the idea. That logic is demonstrated best, he said, by a speaker who will appear later in the program, Paul Blackman of the National Rifle Association (NRA). Mr. Blackman's written statement says that personalized handguns "would not be the first or the most commonly personalized consumer items. Among the personalized items in widespread ownership in America are houses, motor vehicles, and

computers." The NRA concludes, Mr. Henigan went on, that this is a bad idea, because personalization cannot solve social problems. Presumably, the NRA would not object, then, to cars without door locks or without key-operated ignitions and antitheft devices. Most people come to precisely the opposite conclusion, he said. Just as we would be appalled if Ford sold cars with no locks, we ought to be equally appalled that the gun industry sells its products without locks.

Session 3
Impact on Health and Crime

Speaker Presentations

Prof. Philip Cook is the ITT/Stanford Professor of Public Policy at Duke University and a member of the Institute of Medicine, a unit of the National Academies. Among his works is a book coauthored with Jens Ludwig, *Gun Violence: The Real Costs* (Oxford University Press, 2000). Prof. Cook said that one of the things he found most remarkable about the morning proceedings was the significant push by the federal government to develop personalized gun technologies to protect law-enforcement officers and by the New Jersey state legislature to protect children. In the grand scheme of things, he said, those two populations represent only a small part of the problem of the misuse of handguns.

The larger concern is guns that are diverted from their intended purpose into the hands of dangerous individuals who are forbidden by law to have guns. Reducing diversion would reduce gun-related homicides, accidents, and suicides.

Public health statistics give a sense of the scale of the problem. In 1999, there were about 11,000 gun homicides in the United States, almost all caused by handguns. This represents about two-thirds of the total number of homicides in that year. Moreover, there were 187,000 robberies involving a gun, more than one-third of the total number of robberies, and 340,000 gun assaults. There were almost 17,000 gun suicides in 1999, or 57 percent of the total number of suicides. Teenage suicide is of particular concern. Of the 17,000 suicides, 1,100 were younger than 20. In terms of

injuries, there were 29,000 fatalities caused by gun-related injuries in 1999 and 76,000 nonfatal injuries.

A second way of thinking about the magnitude of the issue is to look at the impacts of gun crime. For example, the threat of gun crime imposes a burden on all of us, Prof. Cook said. Fear and anticipation of the possible loss of a loved one translate into costly activities to avoid victimization. Dealing with the consequences of gun crime imposes costs on our criminal justice and medical systems. In many urban neighborhoods, serious violence reduces property values, stops commercial development, and encourages neighborhood flight. The dynamic was illustrated in the 1990s, when a major decline in violence, especially gun violence, coupled with an economic renaissance, led to huge increases in property values in inner cities. Prof. Cook estimated that the costs associated with the criminal use of guns amounts to about $80 billion a year.

No doubt, reducing gun violence could save a lot of money, he continued. Nevertheless, the value of a gun-safety device that adds, say, $30 to the price of a new gun must be balanced against the average additional social burden that additional guns impose on all of us. It is also important to remember that guns have virtuous uses.

Thirty-five to 40 percent of American households own a handgun, typically in conjunction with several other guns (Cook and Ludwig, 1996). The 200 million guns and 70 million handguns in circulation are confined to perhaps 30 million households. Gun-owning households have on the average five guns.

In 1999, 4.7 million new guns, 1.7 million of them handguns, were sold in the United States. There were some 2 to 3 million transactions in used guns. If the purpose of personalization is to reduce diversion, it is important to understand how diversion happens. According to the National Sample of Prisoners, 25 percent of prisoners who had a gun when arrested had acquired it from a retail dealer. In a sample of juvenile offenders, however, only 7 percent said they bought their guns from retail dealers. Buying a gun from a retail dealer and committing a crime with it is relatively rare. Guns usually pass through several sets of hands between retailer and the commission of a crime. Ten percent of prisoners stole their guns; 2 percent took them away from their victims; and about 30 percent bought them on the black market or on the street.

There are four ways a gun can be diverted from a legal user to an illegal user: (1) unauthorized transfer within a household; (2) seizures from victims

by assailants, the so-called take-away phenomenon, a rare event; (3) thefts from residences, vehicles, and commercial businesses; and (4) transfers in the secondary market. Prof. Cook described the last two diversion routes in some detail. There are at least 500,000 gun thefts a year from residences, enough to provide a gun for every gun crime committed in a single year. There are a few million transfers every year in the secondary market. Most of these are perfectly legal, but some are not. The classic straw purchase is when a girlfriend with a clean record buys a gun at a retail store and hands it to her boyfriend, who has a criminal record. There are also sales out of private collections and from states with fewer controls to states with tighter controls.

Conventional personalized technologies, a keyed lock, for example, would do little to prevent the fourth type of diversion, voluntary transfers in the secondary market. When a gun with a keyed lock is sold, the accompanying bracelet or key or ring could simply be handed over so that the purchaser could fire the gun as easily as the seller. A biometric weapon, however, could not be transferred as easily; the gun would have to be reprogrammed. With some technologies, transferring the gun in working order would be impossible.

The personalization could also include a locator built into the gun, a technology that is already used in cars. The Lojack system has led to a steep reduction in vehicle thefts, because it allows law enforcement to track vehicles very easily. Building a signal device into guns would have a remarkable deterrent effect. Even if the signaling device were entirely optional, but perhaps encouraged by insurance companies, the effect could well be to deter theft. That has been the experience with car owners—they pay for Lojack but then get an insurance break. Some miniaturization issues might have to be overcome, but this technology has real potential to stop one very important kind of diversion and make gun theft a lot less attractive than it is now.

Prof. Cook said it would be useful to analyze how these three technologies—key or combination locks, biometrics, and locator signals—match up with the four diversion channels. To what extent would a particular personalization design influence each of these?

A standard key or combination lock design should presumably prevent household diversions, and, if the gun were locked, prevent take-aways. If it were made very difficult to rekey the lock, if rekeying by an unauthorized person would basically destroy the gun, this approach would also prevent

thefts of workable guns. A very similar analysis could be performed for biometric weapons. A gun with a locator device wouldn't prevent household thefts or take-aways, but it might have a substantial effect on theft.

Prof. Cook also raised the issue of "competing" risks. When a new safety technology is introduced, it introduces new, so-called competing risks. The classic example is air bags and seat belts, which reduced old risks but created new ones. For new gun-safety technology, a competing risk might be that, as safer options become available, handgun ownership might rise, thus increasing the overall risk of gun violence. A second competing risk is that some people might get a false sense of confidence, and choose to keep their guns loaded and otherwise unlocked because they think their guns are now safe. Finally, if the locking mechanisms fail, the owner would be prevented from using the weapon during an attack.

Prof. Cook suggested several policy approaches to introducing personalization as a way to address the problem of gun diversions. Handguns with internal locking devices or a built-in geopositioning system could be produced but not required. Another approach would be to require certain groups to carry personalized guns—for instance, people with concealed-carry permits or security guards, who are usually not trained in gun use but are required to carry guns. The third policy option would be to require every new handgun to have an accepted personalization device built in. The result would be a steady increase in the percentage of guns of no interest or use to thieves. It would take a long time for these guns to penetrate the market, but newer handguns are greatly overrepresented in criminal use, so penetration might be fairly rapid.

The fourth and most radical approach would be to require that any conventional handgun being transferred to another owner be retrofitted with an appropriate personalization technology. That would greatly accelerate market penetration.

Social reforms, including gun control, have always been subjected to the same criticisms: futility, perversity, and jeopardy. Futility suggests that reform is hopeless because of the large number (200 million) of guns in circulation. Perversity suggests that smart guns will not fire when necessary, so they would be worse than useless. Jeopardy suggests that requiring smart-gun technology would interfere with our right to own guns. These same arguments have been made for every past social policy reform. But studies of social reforms show that, on balance, they were effective. This suggests

that the correct answer might be that safer guns will mean fewer gun deaths and gun injuries.

Different smart-gun designs would accomplish different purposes. But the larger purpose of all smart-gun technologies should be to reduce diversions, Prof. Cook said. The effectiveness of any particular design will depend not only on the design, but also on the regulations that go with it.

Panel Presentations

Charles A. Moose is chief of police of Montgomery County, Maryland, a major in the District of Columbia Air National Guard, and a member of the adjunct faculty at Montgomery College. Chief Moose said he has carried a handgun for the 27 years he has been in law enforcement, but as a child he never handled a gun. His father had a gun, however, and probably died under the illusion that he had kept it successfully hidden from his children. No one in his household misused his father's gun, but many young people make very poor decisions about the use of family guns, decisions that result in accidental shootings, accidental deaths, and suicides.

In contrast to home- and family-related misuse of handguns, law-enforcement take-aways are a relatively minor problem. Only a small number of law-enforcement officers are killed with their own weapons. A much better reason to pursue smart-gun research would be to stop young people from hurting themselves or others.

One of law-enforcement officers' biggest concerns about smart guns is their reliability. That is the challenge manufacturers must face. Chief Moose said if he and his peers were not convinced that a smart gun would be absolutely reliable every time it is used, they would rather stick with the weapons they already have. There is considerable skepticism in the law-enforcement community about existing gun-safety technologies. A number of law-enforcement agencies ask their police officers to use locking devices on their guns, at least during off-duty hours. His own agency issues the

equipment and encourages its use, and many younger officers, he said, have not only asked for locks but for better locks. But Chief Moose said he doubts that many officers actually use the equipment, and he admitted that he does not lock up his own gun at night. He said he is afraid that, if he needs quick access to the weapon, struggling with a lock will take too much time.

A smart gun would be of most value in preventing gun misuse in the home. Chief Moose noted that homeowners rarely shoot criminal intruders. More often, a criminal completes a crime and may even take the gun away from the victims and use it against them or simply steal it. The idea that guns provide home protection just is not borne out in real-world experience.

Chief Moose said he endorses maintaining a relationship among law enforcement, developers of gun technology, and the public health community. But he repeated that for personalized gun technology to catch on with law enforcement, it would have to be 100 percent reliable. The challenge is not only to design smart weapons but also to sell and market them.

The next speaker, **Paul Blackman,** research coordinator for the lobbying arm of the National Rifle Association, said he knows of no opposition to efforts to develop technologies to prevent unauthorized use of handguns, as long as they are conducted by the private sector. A few gun owners want "such gadgetry," he said, and there is nothing wrong with developing it for them. But he said such technologies will have the effect of making handguns less reliable.

The most obvious limitation in imposing personalization technology is that personalizing consumer products does not prevent unlawful access. Houses and cars have personalized locks, and they are broken into or stolen fairly often. Hacking into personal computers is done for fun and profit. Similarly, personalizing handguns will not prevent misuse but might slow misuse down by a few minutes.

Perhaps the most interesting thing about the effort to develop smart handguns is that proponents of improving handguns rarely have any personal interest in owning a handgun. People who push for safer cars at least ride in cars, he said. But technological gimmickry for guns comes mostly from people who don't like or own guns and who equate the words "gun" and "weapon." That alone makes the notion suspect.

One reason these devices have not been successfully developed for guns is that they don't sell. Gun owners don't want them. Most so-called safety devices make guns less reliable, he said, and will be undone by the consumer. A century ago, Smith & Wesson introduced the grip safety for revolvers.

But purchasers began to undo it, so the company gradually withdrew it, first making it easy to undo, then leaving it off entirely. Much the same is true today for guns sold with magazine interlocks. Most purchasers remove them. It costs only a "buck or two" to put on, and it costs even less to take off, Dr. Blackman said.

The personalized technology that is being talked about will add considerably to the price of a handgun. Any serious personalization being considered today could double or even triple the price of a handgun when you add in the increased cost of liability insurance.

Dr. Blackman said he was opposed to the idea of the federal government imposing the technology and becoming involved in all handgun transfers. He said he also opposed any system of government regulation, approval, or record keeping, which would amount to gun registration. One concern of gun owners is that registration would make confiscation feasible. A few decades ago in Bermuda, after a political assassination, the authorities temporarily called in all registered guns; that temporary confiscation has still not ended. Registration of radios was used by Quisling to confiscate radios in Norway (during WWII) and thus to limit listening to Allied broadcasts. And the Vichy regime in France used registration of Jews as a way to "confiscate" people. One form of personalization, inserting a homing device into guns, would enable police to confiscate non-stolen guns as well, he noted.

Some of the opposition to personalizing handguns, he continued, is based on warranted fears of ultimate goals. Other fears relate to concerns about the reliability of personalized guns. Because most personalization would make handguns unreliable, he said, any attempt to guess their impact on public health and crime is problematic. The question is how unreliable handguns would be, and what would be done by gun owners to keep at least some of them reliable. If unreliability were forced onto all new or all transferred handguns, many buyers would be anxious to restore reliability to their guns.

With respect to personalizing handguns to prevent misuse by children, the NRA shares the concern of the Violence Policy Center that some people who buy these guns would not understand or conform to firearms safety procedures. Moreover, the safety claim would be complicated if only handguns were made childproof, and indeed only new handguns.

Much is simply not known. For instance, Dr. Blackman asked, how would a government willing to force unwanted technology into guns react to owners' efforts to remove or disable the technology? How would gun

owners respond to changes in their guns? How would criminals respond? Currently, gun manufacturers bundle locks with their guns, but these locks will have no impact on the criminal, suicidal, or accidental misuse of guns, because they are easy for criminals and suicides to defeat.

It is impossible to say how many child gun accidents or potential suicides would be defeated by personalization. The restrictions on use provided by personalization would have to be balanced against the possibility that access would be easier, because personalized guns might be more likely to be stored loaded. In addition, children might play with other, unpersonalized guns thinking that now all guns were safe. Similarly, no one knows how many criminals might gain access to unreliable handguns and would be unable to restore their reliability, or whether that would matter. Since most gun-related crimes don't involve shots actually being fired, an unreliable handgun may be as effective a tool for the average criminal as a reliable handgun.

No one knows how police would respond to personalized guns in the hands of children or criminals. Would they be fooled into thinking that newer handguns would fire in the hands of criminals? How many children with access to handguns left lying around because their parents think them childproof might playfully point them at less playful law-enforcement officers?

Would the new technology make handguns unaffordable for the people who most need them for protection and who are already given the least police protection? If so, wouldn't that encourage crime and prevent self-defense? What would be the effect on the cost and availability of used, reliable handguns of having some reliable and some unreliable handguns in the same marketplace?

Tom Diaz, a senior policy analyst at the Violence Policy Center (VPC) and author of the book *Making a Killing: The Business of Guns in America* (The New Press, 1999), was the next speaker. The gun industry is an extremely innovative industry, according to Mr. Diaz. Gun manufacturers have scored some stunning successes through innovation and design. VPC believes that if the gun industry wants to develop and market owner-authorized guns, they should, but they should do it with their own resources, not government funds.

VPC also believes that such technologies should be subject to the same oversight as other American consumer products—regular reviews by an independent agency that balances risks against benefits. The gun industry should also be subjected to the time-honored collective effects of tort litigation.

As has been suggested during this workshop, for the law-enforcement community, a user-authorized gun is a "dog that won't hunt," he said. The community today is not in a buying mode. The real target of the gun industry's efforts to develop personalized handguns is not law enforcement, and has never been law enforcement, he suggested. Introducing a new gun technology to the law-enforcement or defense community first is a means of getting into the civilian market, which can then be much more easily penetrated, and which is orders of magnitude bigger. Anyone interested in selling owner-authorized guns would not be in this business if they think they would only be able to sell to the highly fractionated and extraordinarily skeptical police market. They want to sell to civilians, and they think they can.

It is not entirely accurate to compare user-authorized gun technology to automobiles. A better comparison, Mr. Diaz said, would be with filter-tip cigarettes, which encouraged people to keep smoking cigarettes and destroy their health. Similarly, a smart gun would not do anything to protect American public health. It would encourage large numbers of people who would not have bought handguns otherwise to go out and buy them, believing they are safe. Thus the pool of people who own handguns would expand dramatically.

An owner-authorized handgun poses two risks—a direct risk from the gun itself and an indirect risk related to the pattern of gun ownership in America. Both risks should be studied before anyone assumes that technological success equals epidemiological success.

In terms of indirect risk, gun ownership in America is highly concentrated. Fewer and fewer people now own more and more guns. Moreover, the nature of handguns has changed dramatically in the last quarter century. Twenty-five years ago, most police departments carried six-shot revolvers; today, probably none does. Most police departments have gone through several rounds of rearming and now carry high-capacity, semiautomatic pistols. The same pattern holds true for private owners. In the last 20 years, guns have become far more powerful, with new calibers, bullet sizes, and cross-dimensions. Entirely new calibers have been introduced, such as the Smith & Wesson 40. Gun buyers are seeking out guns with bigger calibers and higher capacity. There is no convincing reason to think that people who purchase smart guns will be any different, and smart guns will probably be of the highest capacity legally allowed. Furthermore, some of the people who are persuaded to buy these guns will already own "dumb" guns, which they intend to keep. That means that, in the same household,

there will be both technologically brilliant and technologically stupid guns available, which will create the serious problem of opportunistic use.

If one examines people's behavior, the argument for technologically smart guns begins to fall apart. Chief Moose's description of what he does and doesn't do with his own gun is a good example. Mr. Diaz said that, as a former gun owner and from his own observations, he doubts that people who buy these guns will keep them in an inoperable mode. The main reason most people buy handguns is for self-defense, and they are not going to buy an implement for self-defense that they make ineffective, by their own actions.

Advocates of so-called smart guns like to draw attention to unintentional shooting deaths of children. Statistically, that occurrence is very small. For 1999, out of 28,874 gun-related deaths, a very small number, about 824, were unintentional. Of those, 158 victims were under the age of 18. If we assumed that every firearm in every household were replaced with a smart gun and that every child under 18 never figured out how to override the safety device, the number of lives saved would still be negligible. Unless you subscribe to the hoary premise that saving one life is enough, the statistics are not persuasive, given the ballooning numbers of new buyers.

Furthermore, almost all unintentional deaths of adults occur during gun-cleaning and hunting activities. In both of those cases, the authorized user is already in control of the firearm.

Suicide is an important category to consider in the argument over user-authorized guns. First, suicide success rates by methods other than guns are far lower. However, authorized gun owners obviously could turn their guns on themselves. Therefore, that category of suicides would not be affected by personalization technology. Teen suicides are often the focus of attention, but many teenagers in America own their own guns. If they are too young to own one legally, their parents often give them one, so they, too, would be authorized users. Much of the gun suicide problem cannot be solved with authorized guns.

The question of homicide and criminality is very dicey. Mr. Diaz said it is his understanding that only a small proportion of homicides results from a criminal intending to kill another person. The preponderance of homicides takes place among people who know each other, and many people who commit homicides are authorized owners. When it comes to criminals who are not the initial authorized owners, the question becomes, as Dr. Cook pointed out, the nature of the technology. Will it be possible to prevent a gun from being transferred?

It is possible to imagine a technological fix to any one of these objections, but the problems are nevertheless very real. To be fair, the presence of a smart gun in the absence of a standard gun would save some lives. But we must balance that against the mass of new owners and new families that would be exposed to the hazards of these guns.

In short, VPC thinks smart guns are a dumb idea, Mr. Diaz said. If the gun industry wants to disprove that, let them. But they should do it on their own dime, and they should be prepared to pay the consequences to the public if they guess wrong in the name of profit.

The last speaker was **Lois Mock,** a senior social scientist and program manager in the Office of Research and Evaluation (ORE) in the National Institute of Justice at the U.S. Department of Justice. She said there is obviously enormous skepticism about the development and use of owner-authorized handgun technology, not only among those on both sides of the gun-control divide, but also within the law-enforcement community.

Ms. Mock said she is concerned that both federal and state legislatures are talking about mandating owner-authorized handguns without considering the possible unintended consequences of such requirements.

One such consequence might be an increase in the market for imported nonowner-authorized handguns, as well as parts for those guns, in response both to legitimate demand from those who want nothing to do with the new technology and to criminal demand.

In addition, all 70 million handguns now legitimately in private hands would suddenly become much more valuable to the criminal element. Most offenders get their guns through secondary markets, which would still be out there. As the number of owner-authorized handguns in circulation increases, the value of guns that aren't owner-authorized would rise, thus increasing the number of household burglaries.

Another unintended consequence of mandating owner-authorized guns might be to increase the use of long guns in the commission of crimes. It doesn't take much to dismantle or saw off the barrel of a shotgun and make it more user friendly and more portable.

The ORE has conducted research for 20 years on issues related to the prevention and control of firearms violence. However, the office has not done social or behavioral research on the impacts of owner-authorized handgun technology, because the technology is still under development. Even so, Ms. Mock said, an affordable owner-authorized handgun could effectively reduce some aspects of gun violence. For instance, personalized

gun technology could prevent accidental injuries and deaths due to impulsive acts by children, and it could cut down on the growing problem of teen suicide.

She noted that the effectiveness of using handguns for self-defense is controversial. The figures in different surveys vary greatly, from less than 100,000 defensive uses per year to several million per year. In some cases, it's not clear how self-defense events are defined. In any case, there is not a one-to-one relation between the defensive use of a handgun and deterrence of a crime.

Sooner or later, owner-authorized handgun technology will be developed. Politically and in the media, it sounds very good, and it will become increasingly difficult for gun manufacturers to refuse to pursue it. Owner-authorized guns could become a valuable tool in reducing certain kinds of injuries and death, but it will not cut down on crimes and violence resulting from the use of available nonpersonalized handguns. Moreover, great care will have to be exercised by those who advocate laws requiring the technology to avoid the potential for increased violence and crime by criminals seeking to acquire pre-law, nonpersonalized handguns.

References

Cook, P.J., and J. Ludwig. 1996. Guns in America: Results of a Comprehensive National Survey on Firearms Ownership and Use. Washington, D.C.: The Police Foundation.

FBI (Federal Bureau of Investigation). 2001. Uniform Crime Reports, Law Enforcement Officers Killed and Assaulted, 2001. Available online at http://www.fbi.gov/ucr/killed/2001leoka.pdf.

Huber, P.W., and R.E. Litan. 1991. The Liability Maze: The Impact of Liability Law on Safety and Innovation. Washington, D.C.: Brookings Institution Press.

NCHS (National Center for Health Statistics). 2002. National Vital Statistics Report 15(5).

Teret S.P., D.W. Webster, J.S. Vernick, T.W. Smith, D. Leff, G.J. Wintemute, P.J. Cook, D.F. Hawkins, A.L. Kellermann, S.B. Sorenson, and S. DeFrancesco. 1998. Support for policies to regulate firearms—results of two national surveys. NEJM 339:813-818.

Weiss, D.R. 1996. Smart Gun Technology Project Final Report. SAND96-1131. May 1996. Available online at www.prod.sandia.gov/cgi-bin/techlib/access-control.pl./1996/961131.pdf (August 4, 2003).

Wirsbinski, J.W. 2001. "Smart Gun" Technology Update. SAND2001-3499. Available online at http://www.prod.sandia.gov/cgi-bin/techlib/access-control.pl/2001/012435p.pdf (August 4, 2003).

Zawitz, W. 1995. Firearms, Crime, and Criminal Justice: Guns Used in Crime. Bureau of Justice Statistics, Selected Findings. NCJ-148201. Available online at http://www.ojp.usdoj.gov/bjs/pub/pdf/guic.pdf.

Appendix A

List of Participants

WORKSHOP ON OWNER-AUTHORIZED HANDGUNS

National Academy of Engineering

June 7, 2003

KEYNOTE SPEAKERS

Philip J. Cook
ITT/ Sanford Professor of Public Policy Studies
Terry Sanford Institute of Public Policy
Duke University
Durham, North Carolina

David Fischer
James Lewis Parks Professor of Law
School of Law
University of Missouri-Columbia
Columbia, Missouri

Donald Sebastian
Vice President for Research and Development
New Jersey Institute of Technology
Newark, New Jersey

John Wirsbinski
Senior Member, Technical Staff
Sandia National Laboratories
Albuquerque, New Mexico

PANELISTS

Paul H. Blackman
Research Coordinator
NRA Institute for Legislative Action
Fairfax, Virginia

Arthur Bryant
Attorney
Trial Lawyers for Public Justice
Oakland, California

Tom Diaz
Senior Policy Analyst
Violence Policy Center
Washington, D.C .

Kevin D. Foley
Vice President Product Engineering
Smith & Wesson
Springfield, Massachusetts

Kenneth D. Green
Director of Technical Affairs
National Shooting Sports Foundation
Frankfort, New York

Dennis Henigan
Director, Legal Action Program
Brady Center to Prevent Gun Violence
Washington, D.C .

Wendy Howe
Program Manager
National Institute of Justice
Washington, D.C.

Lawrence G. Keane
Vice President and General Counsel
National Shooting Sports Foundation
Newtown, Connecticut

Lois F. Mock
Senior Social Scientist
Office of Research and Evaluation
National Institute of Justice
Washington, D.C.

Charles Moose
Chief
Montgomery County Police Department
Rockville, Maryland

Peter Sebelius
Group Leader, Mechanical Engineering
Charles Stark Draper Laboratory
Cambridge, Massachusetts

Dr. Naeem Zafar
President and CEO
Veridicom
Sunnyvale, California

INVITED GUESTS

Curtis Bartlett
Chief, Firearms Technology Branch
Department of Alcohol Tobacco and Firearms
Washington, D.C.

Dennis Carlton
Director, Washington Operations
International Biometric Group
Chantilly, Virginia

Andrew Eros
President
AcciMetrix, Inc.
McKinney, Texas

Jay Heidrick
Attorney
Pottroff, Myers and Ball
Manhattan, Kansas

Karen Kohn
Attorney
Educational Fund to Stop Gun Violence
Washington, D.C.

Jonathan Lowy
Senior Attorney
Legal Action Project
Brady Center to Prevent Gun Violence
Washington, D.C.

Jens Ludwig
Andrew W. Mellon Fellow in Economic Studies
The Brookings Institution
Washington, D.C.

Bryan Miller
Executive Director
Ceasefire New Jersey
Cherry Hill, New Jersey

Victoria W. Ni
Staff Attorney
Trial Lawyers for Public Justice, P.C.
Oakland, California

John V. Pepper
Assistant Professor
Department of Economics
University of Virginia
Charlottesville, Virginia

Susan Peschin
Firearms Project Director
Consumer Federation of America
Washington, D.C.

Robert Pottroff
Attorney
Pottroff, Myers and Ball
Manhattan, Kansas

Brian Siebel
Brady Center to Prevent
Gun Violence
Washington, D.C.

Cary Silverman, Esq.
Shook, Hardy & Bacon L.L.P.
Washington, D.C.

Jennifer Sturiale
Student
Georgetown University
Law Center
Washington, D.C.

Erin Vermilye
Paralegal
Educational Fund to Stop
Gun Violence
Washington, D.C.

Daniel R. Vice
Brady Center to Prevent
Gun Violence
Washington, D.C.

Douglas Weil
Senior Program Officer
Board on Health Promotion
and Disease Prevention
Institute of Medicine
Washington, D.C.

STAFF

Greg Pearson
Study Director and Program
Officer
National Academy of Engineering
Washington, D.C.

Raymond A. Nash, Jr.
Consultant
Andover, Massachusetts

Matthew E. Caia
Senior Project Assistant
National Academy of Engineering
Washington, D.C.

Robert Cherry
NAE Fellow
Idaho National Engineering and
Environmental Laboratories
Idaho Fall, Idaho

Randy Atkins
Senior Public Relations Officer
National Academy of Engineering
Washington, D.C.

Cecile Gonzalez
Public Relations Assistant
National Academy of Engineering
Washington, D.C.

Appendix B

Workshop Agenda

WORKSHOP ON OWNER-AUTHORIZED HANDGUNS

National Academy of Engineering

Green Building
Room 104
2001 Wisconsin Ave., NW
Washington, D.C.

June 7, 2002

7:30 a.m. Continental Breakfast

8:00 a.m. Welcome and Introductions

- ***Lance Davis,*** *National Academy of Engineering*

Plans for the Day

- ***Greg Pearson,*** *National Academy of Engineering*

Session 1: Technology for Owner-Authorized Handguns
Moderator: ***Dixon Dudderar,*** *Lucent Technologies (emeritus)*

8:30 a.m. Keynote Addresses

- ***Donald Sebastian,*** *New Jersey Institute of Technology*
- ***John Wirsbinski,*** *Sandia National Laboratories*

9:15 a.m. Panel
- ***Ken Green,*** *National Shooting Sports Foundation* and *Sporting Arms and Ammunition Manufacture's Institute*
- ***Kevin Foley,*** *Smith & Wesson*
- ***Peter Sebelius,*** *Charles Stark Draper Laboratory*
- ***Naeem Zafar,*** *Veridicom*
- ***Wendy Howe,*** *National Institute of Justice*

10:00 a.m. Q&A

10:30 a.m. Break

Session 2: Liability Concerns
Moderator: ***Mark Behrens,*** *Shook, Hardy & Bacon L.L.P.*

10:45 a.m. Keynote Address
- ***David Fischer,*** *University of Missouri*

11:15 a.m. Panel
- ***Larry Keane,*** *National Shooting Sports Foundation*
- ***Arthur Bryant,*** *Trial Lawyers for Public Justice*
- ***Dennis Henigan,*** *Brady Center to Prevent Gun Violence*

12:00 p.m. Q&A

12:30 p.m. Lunch

Session 3: Impact on Health and Crime
Moderator: ***Lance Davis,*** *NAE*

1:30 p.m. Keynote Address
- ***Phil Cook,*** *Duke University*

2:00 p.m. Panel

- ***Charles A. Moose,*** *Montgomery County Department of Police*
- ***Paul H. Blackman,*** *National Rifle Association*
- ***Tom Diaz,*** *Senior Policy Analyst, Violence Policy Center*
- ***Lois Mock,*** *Department of Justice*

2:45 p.m. Q&A

3:15 p.m. Comments from Invited Guests
Moderator: ***Lance Davis,*** *NAE*

4:15 p.m. Summary and Closing Remarks
Lance Davis, *NAE*

4:30 p.m. Adjourn