Personalized Firearms
and Electronic Safety Devices

Perspectives

These four papers have been commissioned by the Small Arms Survey to make available a variety of perspectives on existing and prospective firearm technologies, to inform discussions at the conference ‘Smart Technology in SALW Control: Civilian Protection, the UN-POA, and Transfer Control (SmartCon)’.

The findings and views presented in these papers do not necessarily reflect those of the Small Arms Survey.
# Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>PREFACE</td>
<td>4</td>
</tr>
<tr>
<td><strong>Electronic Firearm safety devices</strong></td>
<td>6</td>
</tr>
<tr>
<td>Introduction</td>
<td>6</td>
</tr>
<tr>
<td>Characteristics of FSDs</td>
<td>6</td>
</tr>
<tr>
<td>Use of FSDs</td>
<td>7</td>
</tr>
<tr>
<td>Mechanical FSDs</td>
<td>7</td>
</tr>
<tr>
<td>Electronic FSDs</td>
<td>8</td>
</tr>
<tr>
<td>Statutory regulations for the use of FSDs</td>
<td>10</td>
</tr>
<tr>
<td>FSD use in least-developed countries</td>
<td>10</td>
</tr>
<tr>
<td>Conclusion and outlook</td>
<td>12</td>
</tr>
<tr>
<td>About the authors</td>
<td>12</td>
</tr>
<tr>
<td>References</td>
<td>13</td>
</tr>
<tr>
<td><strong>German Gun Law: The Introduction of Electronic Firearm Safety Devices (FSD)</strong></td>
<td>14</td>
</tr>
<tr>
<td>Retrospective</td>
<td>14</td>
</tr>
<tr>
<td>Significant amendments introduced in the 2009 Weapons Act</td>
<td>15</td>
</tr>
<tr>
<td>Public discussion after the passing of the new Weapons Act and applications for further bans</td>
<td>16</td>
</tr>
<tr>
<td>Plans to tighten the Weapons Act by using fingerprint identification technology to lock firearms</td>
<td>16</td>
</tr>
<tr>
<td>The potential of the Weapons Act to bring storage safety/firearms and ammunition safety in line with current technology</td>
<td>17</td>
</tr>
<tr>
<td>Perspectives</td>
<td>21</td>
</tr>
<tr>
<td>About the author</td>
<td>21</td>
</tr>
<tr>
<td>References</td>
<td>21</td>
</tr>
<tr>
<td><strong>Key Perspectives and Insights on Personalized Guns</strong></td>
<td>24</td>
</tr>
<tr>
<td>Introduction</td>
<td>24</td>
</tr>
<tr>
<td>The need for personalized guns</td>
<td>24</td>
</tr>
<tr>
<td>The background and history of mechanical firearm personalization technology</td>
<td>25</td>
</tr>
<tr>
<td>Early experiments to electronically personalize handguns</td>
<td>27</td>
</tr>
<tr>
<td>US legislative and litigative activity</td>
<td>28</td>
</tr>
<tr>
<td>Current technical options for personalizing guns</td>
<td>29</td>
</tr>
<tr>
<td>Current perspectives</td>
<td>30</td>
</tr>
<tr>
<td>About the author</td>
<td>32</td>
</tr>
<tr>
<td>References</td>
<td>32</td>
</tr>
<tr>
<td><strong>Using Computer Technology to Increase Gun Safety</strong></td>
<td>35</td>
</tr>
<tr>
<td>Introduction</td>
<td>35</td>
</tr>
<tr>
<td>Background: defining the problem</td>
<td>36</td>
</tr>
<tr>
<td>Technology to personalize guns</td>
<td>36</td>
</tr>
<tr>
<td>Risks, limitations, and concerns</td>
<td>38</td>
</tr>
<tr>
<td>Inside the DGR prototype</td>
<td>40</td>
</tr>
<tr>
<td>Reducing incidents and accidents with personalized guns</td>
<td>42</td>
</tr>
<tr>
<td>Future directions in personalized guns</td>
<td>42</td>
</tr>
<tr>
<td>About the author</td>
<td>43</td>
</tr>
<tr>
<td>References</td>
<td>43</td>
</tr>
</tbody>
</table>
PREFACE

Personalized Firearms and Electronic Safety Devices: Perspectives

Pierre Gobinet, Small Arms Survey

Firearm safety has traditionally relied on mechanical systems. External safety devices, such as safes and cable locks, are used to address unauthorized removal, and to prevent theft. Integral mechanisms insure user-safety once the weapon is in hand. For the popular semi-automatic handguns, for instance, integral safety features include standard manual hammer blocks, de-cocking levers, and trigger- or magazine-disconnect safeties. Mechanical safety (external or integral) systems are efficient, but have shown limited capacity to prevent diversion or minimize accidental gun deaths, youth suicides, assaultive and homicidal shootings.

Initial interest in smart—or electronically personalized—firearm safety technology can be traced back to the mid-1990s and early 2000s, when several US manufacturers received federal grants to explore and test personalized safety options. For a number of reasons none of the prototypes was ever commercialized. Today, civilian customers and law enforcement practitioners still perceive integral gun safety as mechanical, and express a deep and general mistrust of integrated electronics. Manufacturers do not want to be associated with ‘smart’ gun R&D efforts for fear of jeopardizing their corporate image and losing their customer base.

Yet there remains policy and industry interest in personalized integral and external firearm safety technology. Friendly-fire accidents, such as shootings of police officers with their own service firearms, periodically revive debates about the feasibility of ‘smart’ handguns that incorporate electronic technology such as RFID chips, fingerprint recognition, or magnetic rings to restrict access and use of a gun to a specific shooter. In the U.S., some States anticipated these trends and tasked oversight bodies to monitor the development of personalized handgun technology and to report on its availability on the retail market. In Europe, some companies are investing in both personalized gun and gun-storage technologies, and are currently approaching gun manufacturers worldwide to promote their systems.

In order to dispel myths and shed light on this sensitive debate, in June 2013, the German Federal Foreign Office and the Bonn International Center for Conversion will organize a conference on smart technologies for small arms control in Berlin. This conference, and the associated publication, targets a wide audience from various communities: academic researchers, gun control advocates, industry representatives, stockpile management practitioners, law enforcement officers, hunters, and sport shooters.

To support this event the Small Arms Survey solicited four prominent stakeholders representing academia, industry, R&D and government to author independent, non-commercial, and policy-relevant texts reflecting the ‘smart gun’ debate in Germany and the United States.

The first and second papers are dedicated to electronic firearm safety devices (FSD), with a focus on Germany. In the first paper, Günter Maximilian Hefner and Karl Friedrich Giebel
describe the typology and technical potential of electronic FSDs. Jörg Schönbohm, former Chief of the German Army and member of government, emphasizes the role of political will, and provides his perspective on the German Gun Law’s acknowledgement, acceptance, and promotion of electronic FSDs. The third and fourth papers are dedicated to personalized firearms, with a focus on the United States, where much of the legislative activity and development have occurred. Stephen Teret discusses the need for personalized guns, as well as the history, technology, public acceptance, politics, and law related to such guns. Michael Recce details the Dynamic Grip Recognition (DGR) biometric gun that was developed by the author and his colleagues at the New Jersey Institute of Technology (NJIT).

The Survey expects this compendium to raise questions among the public, news media, and non-governmental organizations as to why electronic gun safety systems are not yet a reality. The publication is also expected to provide the German Federal Foreign Office with additional leverage to reinvigorate the debate on personalized guns in civilian, law enforcement, and military circles.
Electronic Firearm safety devices

(Translated from German)

Günter Maximilian Hefner and Karl Friedrich Giebel

Introduction

Traditionally, the development of handguns has focused on the technical function of the gun itself as a weapon. Safety-related requirements are usually restricted to ensuring that it functions in unfavourable conditions or preventing unintentional activation or firing. Examples of this are anti-drop locks as formulated in Germany’s 2008 Technical Directive (Germany, 2008) or special trigger systems that are designed to ensure that the weapon can only be fired if the trigger is used intentionally and correctly (e.g. Glock, n.d.).

However, Glock (n.d.) unintentionally mentions the fundamental problem with user-friendly safety systems: ‘All three pistol safeties are deactivated when the trigger is pulled—and automatically activated when it is released.’ Added to this are police authorities’ increasing demands for ease of use and lower trigger weights. The consequence is that modern handguns are ‘child’s play’ to operate, and therefore represent a correspondingly greater potential hazard if they end up in the wrong hands.

Also, because of the opinion of gun users and their representatives that there should be no device in the weapon that prevents it from being used rapidly and reliably (NRA, 2002), integral safety devices in firearms are still not widespread either in guns used for self-defence or in sports or hunting guns.

Instead, the safety issue has been externalized, e.g. by using additional devices to compensate for the lack of built-in firearm safety. Examples of this are gun safes and safety holsters.

Firearm safety devices (FSDs), which have also been on the market for some time, offer protection above and beyond these special cases, which can be enhanced further if modern electronic authentication and communication processes are used.

Characteristics of FSDs

Unlike devices such as gun safes and holsters, FSDs are fitted to the weapon itself. In principle they prevent it from being used, e.g. such as the trigger being pulled.

The weapon can only be used once the FSD has either been completely removed or has been set so that this function is enabled again. For the latter purpose the FSD is an authorization device.

A fundamental characteristic of an FSD is the definition of the safety level at which it is set. For this, appropriate directives and test criteria are usually established. Examples of this are the Technical Directive for Blocking Systems issued by the German Federal Ministry of the Interior,
Use of FSDs

Of the approximately 875 million small arms in circulation worldwide (Small Arms Survey, n.d.), only a small fraction is in use at any one time. Both privately and publicly owned (police, military) firearms are in most cases stored so that they are not immediately accessible or transportable. It is particularly in cases where the lawful and responsible user cannot regulate third-party access because of his/her absence that a secure technical device is required to protect the weapon from non-authorized use.

In particular, an FSD must be capable of covering the following scenarios:

- the transportation and shipping of firearms;
- temporary storage, for instance when travelling or at events;
- the storage of firearms under conditions where there is no access to facilities such as gun safes;
- the provision of additional firearm safety in especially high-risk situations (such as uninhabited buildings, storage of a large number of weapons, etc.); and
- quick and easy activation of the gun safety device when use of the gun is over (e.g. at sporting events).

Mechanical FSDs

Weapons are not usually designed specifically to accommodate an FSD, so that certain general characteristics of firearms can be used as a safety device independent of model. A typical example of this is the trigger lock fitted to the trigger of a handgun (see the example on the left in Figure 1). These locks are generally standardized and are designed to prevent activation. They include a cable lock, which is passed through the magazine and the ejection port to prevent the magazine from being loaded and the weapon from being closed (see Figure 1, right).

Figure 1: Trigger lock and cable lock
Safety systems that go beyond this rather rudimentary protection usually block certain components of the gun, which cannot be created or reconstructed without specific technical knowledge of firearms. These components usually include the barrel, the breech, and the grip in the case of handguns.

Current safety levels demand that any improper deactivation or removal of the FSD should result in the destruction of the affected components, rendering the firearm permanently unusable.

Examples of this are safety devices that are fully inserted in the chamber or barrel and therefore cannot be manipulated. Forcible removal destroys the chamber so that the weapon can no longer be loaded.\(^1\)\(^2\)

This category also includes safety devices that are used in place of the magazine or surround the gun so that it is not possible to access the functional elements.\(^3\) However, the design of this type of safety device typically has to be customized to the firearm model being made safe, so that manufacturers are limited to a few common models and no modifications may be made to standard guns.

A further characteristic of safety devices that operate purely mechanically is that they are not able to fulfil the standard requirements of modern safety concepts. These include:

- the option of integrating and combining mechanical devices with various authorization processes (token, password, biometric);
- hierarchical authorization;
- traceability and logging functions; and
- networking and remote availability.

Because of this, particularly in the politically and socially sensitive area of the availability and use of firearms, existing FSDs are being upgraded so that they can offer these functions.

**Electronic FSDs**

Upgrading the FSD concept to feature electronic components is a challenge in many ways.

For example, the use of such a system in a compact handgun requires a high integration density, while the requirements for functional safety and the safe manipulation of the system are orientated to the requirements of the handgun itself. The components to which this particularly applies are the user interface, authentication device, actuators and sensors, and power supply.

There are only limited possibilities for using derivations from related areas of safety technology such as automotive or defence technology, because in these areas the acceptance of electronic

\(^1\) E.g. see [http://omegagunlock.com/productline.htm].
\(^2\) E.g. see [http://www.gunvault.com/gun-locks/magvault.html].
\(^3\) E.g. see Sportlock LLC, [https://www.sportlockllc.com/].
safety and control systems is traditionally higher and has increased significantly in the last 20 years.

So the design of electronic safety systems for handguns can only be planned on the basis of STANAG criteria\(^4\) or requirements from the functional safety standard IEC 61508.\(^5\) Specific requirements for electronically controlled retrofittable firearm safety systems are currently not known anywhere in the world, in the form of either legislation or any other technical directives.

By comparing the FSD directives quoted above (none of which stipulates electronic systems, although all explicitly permit them) it is possible to derive the following generally applicable safety standards:

- personalized locking mechanisms (PIN, biometrics, or physical key);
- 30 minutes’ resistance against tools in common use (including drills, lathes, milling machines, angle grinders, electrical mounted grinding points, etc.);
- EMC interference immunity in accordance with IEC 61000-4-3;
- tensile strength in accordance with a standard in common use (e.g. DIN EN 1627, DIN EN 1630, DIN EN 1143-1);
- resistance against compressive force and traction up to 15 kN; and
- resistance against thermal stress up to 800°C for more than 15 minutes.

However, only a few of the products currently on the market in this sector provide a market analysis based on these criteria (e.g. see Armatrix, n.d.). The reason for this, as well as the lack of legal acknowledgement of the products, is the fact that the purchase price is still comparatively high and small-gun users are hesitant to accept electronic safety systems.

![Figure 2: Electronic FSD: Armatix Quicklock](http://nsa.nato.int/nsa/)

However, in all three areas conditions seem to be changing at the moment.

In the light of the political discussion about more stringent firearms legislation in the United States and Europe and increased awareness of the misuse of weapons, politicians in the world’s

\(^4\) [http://nsa.nato.int/nsa/]

\(^5\) [http://www.iec.ch/functionalsafety/].
largest firearms market, the United States, appear to be rethinking their approach to the issue (Washington Post, 2013). However, now that it has become clear that it is not possible to restrict the sale of firearms by referring to laws, the focus of the discussion is changing to the regulations for storage and handling.

Furthermore, a higher level of acceptance of retrofittable electronic safety systems already seems to be going hand-in-hand with the increasing acceptance of electronically controlled and locked weapons (‘smart guns’).

In combination with the emergence of more manufacturers in this new market sector in the foreseeable future, this will lead to a narrowing of the price difference between purely mechanical systems and electronic FSDs, with the result that the latter will become more widespread.

---

**Statutory regulations for the use of FSDs**

Currently (2013) retrofittable FSDs are mostly legally recognized in Germany, Canada, and some US states. Outside these areas some regional by-laws are in existence (for instance, in some US counties, but also specific legislation in South America). The reason for this is that in many states gun legislation is a matter for local police and municipal laws.

FSD use in Germany is required only in cases where the firearm is inherited by someone who does not have a possession permit recognized by the German Weapons Act (Germany, 2002, sec. 20). The reason for this regulation is that the new owner, who may not be a firearms expert, should not be technically in a position to load and use the weapon. For this reason the safety device is installed and uninstalled by a person authorized to do so (i.e. as holder of a weapons manufacturer’s or dealer’s licence). Technical devices (e.g. specific code programming and storage of the code at a trusted location) ensure that authority to deactivate the weapon cannot be transferred to the gun owner.

Specifically in the US state of California it is compulsory by law that every gun sold also has an FSD (California DoJ, 2013). To this end, a wide range of regulations apply to its testing and licensing. Other states, such as Maryland, New Jersey, and New York, follow California’s laws, having either adopted them as they stand or adapted the licensing procedure.

The legal regulations for the storage, transport, and handling of weapons in Canada require that weapons are only transported if a permanent safety device or FSD is used (Canada, 1998).

---

**FSD use in least-developed countries**

The use of FSDs in so-called least-developed countries (LDCs) is advisable for many reasons, and if used consistently could help to restrict illegal weapons trading and the widespread possession of guns.

As shown in red print in Figure 3, the transition of weapons from the legal outer circuit into the illegal inner circuit is either prevented or seriously and lastingly impaired.
Weapons with built-in safety devices can neither be loaded nor misused if stolen. Since many LDCs do not have an infrastructure that is considered adequate for safe firearms storage, and large-scale gun theft is an everyday occurrence in some areas, it would be urgently advisable for all firearms in LDCs to have individual safety devices.

![Image of Life cycle of a gun](https://example.com/life-cycle-gun.png)

Figure 3: The effect of FSDs in the life cycle of guns (Source: Saferworld, 2012)

Weapons transport in the context of disarmament projects would no longer be at risk of arbitrary attacks with violent consequences. It would also no longer be necessary to consider the available technical infrastructure of buildings with regard to gun safety for small arms and light weapons stockpile management.

The concept of FSDs was presented to representatives of the local small arms control commissions of the Economic Community of West African States and received enthusiastically at a conference in Abidjan in November last year on the subject of small arms and light weapons. The benchmark data for an initial field trial in the Ivory Coast is available and this is currently in the project-planning phase.

In projects such as this it is important to pay particular attention to providing users with efficient and lasting training, because generally speaking they will probably have no or insufficient experience of handling FSDs.

The question inevitably arises as to how projects of this kind are to be financed, as well as their costs in comparison with alternative storage of firearms in conventional freight containers. Of course, the budgets required will be higher at first. The question that donor countries have to ask themselves in these situations is how much more damage can be prevented by individually locking the weapons concerned.
Conclusion and outlook

FSDs—both in the traditional mechanical format and the electronic version—have the potential to improve gun safety in areas that could not previously be covered by standard safety devices. In particular, the first electronic safety devices available on the market that feature enhanced authentication, logging, and integration functions have the potential to adapt to requirements in a way that cannot be achieved with other procedures.

The use of firearm safety systems is traditionally associated with the fulfilment of legal requirements. This applies both to the user perspective and the technical requirements of FSDs. In this regard it is to be expected that individual countries will be increasingly responsible for introducing clear legislation. Experience from the United States and Germany shows that products with specific characteristics become marketable as a consequence of legislation. This specifically applies to electronic safety systems as a newly emerging product.

As regards the immediate future, it is expected that existing products will be adapted to suit the different target markets more closely (e.g. authorities, private individuals, and the military). It can be assumed that FSDs could increasingly form an interface with higher-level systems or become integrated with them, as has been the case with developments in automotive and communication technology.

This would then affect solutions for weapons organization, the assignment of authorization, localization, and time control, as well as the classic areas of firearms transport, storage, and use.

About the authors

Maximilian Hefner, Managing Director and CMO at Armatix GmbH

Mr. Hefner oversees the sales and corporate marketing functions for Armatix GmbH. Over the past 20 years, Hefner has held a variety of leadership positions at different industries like factory automation, cell phones and smart cards, including a 5 year assignment as General Manager in Hong Kong and Singapore. Hefner graduated with a Master degree (Dipl.-Ing.) in Mechanical Engineering from Technical University Munich/Germany.

Dr. Karl-Friedrich Giebel, Head R&D at Armatix GmbH

The PhD physicist has been with Armatix (at that time still SimonsVoss AG) since 2003. As head of research and development he is responsible for the design of digital weapon safety systems like integrated smart gun devices or retrofit solutions. Before joining Armatix he worked as technical engineer, software designer and project manager in the sector of image processing, optical data analysis and automation for one of the leaders in the field of industrial measurement technology.
References

Armatrix. n.d. ‘Quicklock: The First Mechatronic Gun Safety the New Multi-gun Storage Device.’ <http://www.armatix.us/Quicklock.144.0.html?&L=7>


Retrospective

The current German Weapons Act regulates the way in which weapons are handled. Internationally the Act is considered one of the most stringent in existence (Breitenbach, 2010).

The 1976 German Weapons Act was replaced on 1 April 2003 by two new laws: the Weapons Act and the Ammunition Act. An amendment to the Weapons Act came into force on 25 July 2009 (see below). The Weapons Act serves to protect public safety and order, and regulates the handling of weapons and ammunition, i.e. acquisition, possession, carrying, manufacturing, and dealing. The Ammunition Act regulates the safe use of weapons and ammunition.

The Weapons Act was amended after the Winnenden massacre on 11 March 2009, in which the 17-year-old perpetrator used a large-calibre pistol to kill 15 people and himself at a school in Baden-Württemberg. According to police investigations, the firearm belonged to the offender’s father, who owned the gun legally as a sports marksman, but did not keep it in a gun safe as required by law, so that the offender had unauthorized access to the weapon.

In 2009 at a school in Winnenden a 17-year-old perpetrator shot 15 people and himself using his father’s firearm, prompting an amendment to the German Weapons Act. Photo: Oliver Lang / DDP / AFP
In their responses to the massacre, the Christian Democratic Union (CDU)/Christian Social Union (CSU) coalition and the Police Union (GdP) at first rejected criticism of the existing Weapons Act, because they felt that the storage of firearms was already adequately controlled by law. According to Wolfgang Dicke, the GdP weapons expert, the ‘weak point of the Weapons Act is the people themselves who do not observe the law’ (Spiegel Online, 2009).

However ‘the debate among the general public after this school massacre forced the coalition of the CDU, CSU and SPD [Social Democratic Party] to make some changes to the Weapons Act in July 2009’ (Germany, 2010a, p. 1, para. 2). Proposals from political parties ranged from central storage of weapons and ammunition to a ban on large-calibre firearms, the biometric locking of weapons and a total ban on firearms ownership (GDP Newsletter, 2009, pp. 6–20; Germany, 2009a; 2009b).

On 31 May 2009 the coalition announced amendments to the Weapons Act that it had drawn up in collaboration with a national/regional working group set up specifically for this purpose. The objective of the amendments was to prevent unauthorized access to legal weapons and to make it more difficult for minors to access offence-relevant weapons (CDU/CSU, 2009).

On 17 June 2009 the Free Democratic Party (FDP) faction issued a draft resolution on the Weapons Act amendment that called for improvements in its enforcement and an evaluation of the changes made in 2008. On 18 June 2009 the German Bundestag (parliament) passed the new gun law without further changes to the draft (Die Welt, 2009). The Bundesrat (Federal Council) passed the amendment on 10 July 2009.

**Significant amendments introduced in the 2009 Weapons Act**

The following significant changes were introduced in the amended Weapons Act:

1. Gun owners have to permit checks of their accommodation, even when there is no reasonable doubt that they are storing weapons safely. On 22 July 2010 the Fördervereinigung Legaler Waffenbesitz e.V. (Association to Support the Legal Possession of Weapons) lodged an objection to this amendment in the Federal Constitutional Court claiming an infringement of the constitution and an associated infringement of the ‘Inviolability of the Home’ clause enshrined in Article 13 of the German constitution (Süddeutsche.de, 2010a). The court dismissed the case on 6 February 2012 (Germany, 2012a).

2. Intentional infringement of the obligation to store firearms appropriately is no longer classed as merely an administrative offence, but is now a criminal offence punishable with a fine or a prison sentence of up to three years (Germany, 2009c, para. 52(a)).

3. The introduction of a continual needs test as well as new rules for exceeding the regulated number of weapons per owner: approval for owning more than three semi-automatic long firearms and more than two multiple-shot handguns will in future only be granted if the gun owner regularly takes part in shooting competitions.

4. According to a European Union (EU) directive dated 21 May 2008, by 2014 a computer-based central or decentralized gun register must have been introduced in every EU country.
Germany had already implemented this centrally by 1 January 2013 with the Weapons Act amendment of 2009 (Germany, 2012b).

The amendment to the Weapons Act gives legislators the opportunity to stipulate the use not only of safety containers for storage, but also of specific safety systems for large-calibre shotguns (Germany, 2009c, para. 5).

---

**Public discussion after the passing of the new Weapons Act and applications for further bans**

The amendments to the Weapons Act passed after the Winnenden massacre were not sufficient for the Bündnis90/Die Grünen faction. On 16 June 2009 they applied for further bans and conditions as follows: the central storage of firearms and/or ammunition in gun club buildings, a ban on large-calibre shotguns, a ban on high-penetration ammunition, a general limit on private firearms possession, a central electronic weapons register, and permits for purchasing and owning blank-firing guns (Germany, 2010b).

The attacks in Norway in 2011, in which Anders Breivik killed ten people with a car bomb and shot 69 people dead on a holiday island with a semi-automatic weapon, caused the Bündnis 90/Die Grünen faction to submit draft legislation for a ban on military-style semi-automatic firearms on 9 November 2011 (Germany, 2011).

Both applications were discussed at a public hearing on 21 May 2012 before the Federal Internal Affairs Committee and were heavily criticised by experts (Germany, 2012d). Representatives from the police and public prosecutor emphasized that it was illegal weapons and not legal ones that were the problem. All the experts agreed that centralized storage would pose more of a public threat than storage in homes. They further agreed that the assumption that fewer weapons would result in higher levels of public safety was unfounded.

---

**Plans to tighten the Weapons Act by using fingerprint identification technology to lock firearms**

In April 2009 the then-interior minister, Wolfgang Schäuble (CDU), announced proposals to require weapons to be locked so that they could only be unlocked by their owners. ‘There are some interesting technical possibilities’, he said in an interview with the Rheinische Post, referring to a locking device that could only be released using fingerprint identification technology. He also said that regulations for storing weapons in private homes should be tightened. Schäuble’s ministry had already initiated talks with the German states, as well as with gun clubs and hunters: ‘We want results by the next interior ministers’ conference at the start of June 2009’, he said. ‘Should it be the case that we have to change laws to achieve this, then we will do so before the end of this parliamentary term’ (Focus Online, 2009).

At the time a system to lock firearms using fingerprint identification technology that worked by inserting a locking element into the chamber to make the weapon unusable was already on the
market. The gun could only be unlocked by providing the fingerprint via a small electronic device linked to the locking element. It could also be unlocked using a PIN number.

At the same time Berlin interior senator Erhart Körting (SPD) spoke in favour of making this type of safety device compulsory by law. Thereafter the national and regional ministers of the interior convened at their spring conference in Bremerhaven on 3–5 April 2009, where the amendment of the Weapons Act was on the agenda.

However, although the Weapons Act was passed in 2009, the corresponding adaptations to bring the regulations in line with current technology for intelligent locking of weapons have so far not yet been drawn up. It would therefore seem that gun safety is only discussed in Germany when there are specific reasons to do so, for instance the massacres in Winnenden and Erfurt. After a while these discussions are superseded by other current affairs and are quickly forgotten. Gun safety is not a current topic and in principle nothing has changed, although there are plenty of reasons for this to happen. These constant changes in national priorities regarding gun safety have not resulted in any changes to the law. However, the German Bundestag has acknowledged the risks associated with firearms misuse and has issued a resolution asking the Federal minister of the interior to investigate the viability of modern gun-safety technology. The minister investigated such technology and decided that there was no need to act yet, as it was still at an early stage of development and no final decision could be made.

For this reason nothing has changed thus far and the old principle of gun law still applies, which states that the only way of preventing a gun’s misuse is to prevent its removal by protecting it against theft and other illegal forms of removal. Accordingly, an adequate security device should be employed to prevent loss within the domain of the person authorized to be in possession of these dangerous items. So the focus is on the abstract offence, because in the eyes of the law it is not possible to directly prevent the specific offence of misuse. The reason for this is that effective systems to prevent unauthorized use did not exist at the time the 2009 law was passed. Nevertheless, the legislative authority envisioned the prospect of effective safety devices to prevent misuse, and section 36, paragraph 5 of the Weapons Act allows for new technical developments to be taken into account at the administrative level when statutory instruments are issued (discussed below) (Germany, 2009c).

The potential of the Weapons Act to bring storage safety/firearms and ammunition safety in line with current technology

**Weapons Act, section 36, paragraph 5**

**Power to issue statutory instruments**

Within the scope of the power to issue statutory instruments created in 2009 and standardized in section 36, paragraph 5, the Weapons Act states the following:

---

6 The Erfurt massacre occurred on 26 April 2002 at the Gutenberg Gymnasium. The gunman, 19-year-old expelled student Robert Steinhäuser, shot and killed 16 people.
(5) The Federal Ministry of the Interior shall be authorized, after consulting the stakeholders, to issue statutory instruments with the assent of the Bundesrat and taking into account the state of the art, the type and number of weapons and ammunition, and the locality, waiving the storage requirements or stipulating additional requirements concerning the storage or security of weapons. Such orders may

1. define specifications for technical security systems to prevent the unauthorized removal or use of guns,
2. require the retrofitting or replacement of existing security systems,
3. require guns to be equipped with mechanical, electronic or biometric security systems.

In light of this, a Bundestag resolution of 18 June 2009 (Germany, 2009d) requested the government to:

- provide an overview of options for improving the safety of weapons and ammunition—both existing and in development—to protect against loss or unauthorized access;
- provide advice on effective solutions for improving the safety of weapons and ammunition as soon as possible in conjunction with those affected (including manufacturers and gun clubs); and
- implement such a solution as promptly as possible by way of an appropriate regulation.

Content

Section 36, paragraph 5, clause 2(1) refers to the requirements of technical safety systems. It makes provision for both the option of an additional safety device to protect against improper use alongside the existing safe storage regulation and the replacement of the existing storage regulation with a system that simultaneously protects the firearm against removal and misuse. What is new is that these safety systems not only prevent the unauthorized use of firearms, but also their unauthorized removal. In perspective, this means that safety systems could take the place of secure storage locations or be used in conjunction with them.

Clause 2(2) is new and its objective is to keep safety systems up to date with current technology by permitting legislation to require that specified systems either have to be upgraded or even replaced completely if upgrading is insufficient.

Clause 2(3) is also new and applies to firearms. It makes it possible to define mechanical, electronic, or biometric safety systems, as well as a combination of these types, such as mechatronic systems.

State of technology in relation to the Weapons Act, section 36, paragraph 5

Technology has now achieved the level of development required by section 36: tested and certified safety systems to combat both misuse and removal are available for almost all privately owned firearms. This would make it possible to step up the security level of gun storage and protection against misuse. The possibility of tightening up gun law now exists with this power to issue statutory instruments.
Technical solutions for locking weapons intelligently

What technical solutions are currently available and to what extent can they be relied on?

The basis of all upgradeable safety systems currently on the market is the so-called locking device. This mechatronic device consists of high-precision mechanical components and an electronic control unit. The size of the locking device corresponds exactly to the calibre of the gun being secured. The device is inserted into the barrel of the gun, where slight pressure causes it to lock in place in the chamber. This takes a fraction of a second and cannot be reversed without the correct authorization. This type of safety device means that firearms and ammunition can be stored and transported together, because it is not possible to load a cartridge while the safety device is in place.

The firearm is safer with a locking device in its chamber than it would be in a safe. The locking device cannot be removed from the chamber by force: trying to do so would destroy the barrel of the gun and render it unusable. Legitimate users have to be authorized to remove the locking device via a control unit, e.g. by entering a freely programmable PIN number or using the electronically stored fingerprint of an authorized user. Once the authorized user has entered the release PIN and/or provided their fingerprint, the control unit and the locking device exchange encoded information. The release process takes no longer than the securing process.

It does not yet seem to be clear to some politicians and parts of the civil service that modern technology can provide a system that protects firearms against both removal and misuse. Changing attitudes is the main problem, as well as the fact that lawmakers and civil servants need to be made aware of the existence of modern technology and how it works. Despite the announcement from Interior Minister Schäuble in 2009 (Focus Online, 2009), politicians have since taken no steps towards authorizing the issue of secondary regulations in terms of section 36, paragraph 5 of the Weapons Act.

Weapons Act, section 36, paragraph 2

Containers with equivalent safety ratings

The following regulation was also introduced in 2009:

(2) Guns not exempted from the licence requirement and banned weapons shall be stored in a container that complies at least with the DIN/EN 1143-1 standard, resistance grade 0 (as of May 1997) or an equivalent; in particular, a security grade B container in accordance with VDMA (as of May 1995) shall qualify as equivalent. Up to ten long firearms shall be deemed to be securely stored if they are stored in a security grade A container in accordance with VDMA 24992 (as of May 1995) or an equivalent standard of another EEA member state. Rooms secured in a comparable manner shall be deemed equivalent.

In accordance with section 36, paragraph 2, clause 1, firearms requiring a licence may be stored not only in containers that comply with the standard DIN/EN 1143-1, but also in safes with the same safety rating. There is a legal fiction that a VDMA (German Engineering Federation) safe in particular is seen as fulfilling the requirements of this clause of the Act. These gun safes are particularly commonly used because of their significantly more lightweight design in comparison
with the zero theft impediment safe, for which alternatives were practically unavailable until recently. Various tests commissioned by an official test institute have shown that these safes can be opened in less than four minutes with tools that can be bought in a hardware store. This would then give unauthorized persons free access to the fully functioning firearms and ammunition contained in the safe. The surprising thing is that people know about this safety loophole, but it is accepted because an alternative is not considered to be available.

**Current state of technology in terms of Weapons Act, section 36, paragraph 2**

Because of this loophole, companies in the market have developed safety systems based on modern technology that meet the required standards and even outperform them. Until very recently these safety systems were undergoing checks by the Federal Ministry of the Interior and have now been made available on the market.

This means that gun owners have another storage option available in addition to currently available safes—an option that conforms to the law and is at least equivalent to existing storage products. For instance, one intelligent stationary system that is already on the market secures all short guns—including their magazines—and connects them to centralized monitoring systems on request. Depending on the requirements, holders can be mounted on a table, wall, or floor in buildings, cars, or special-purpose vehicles of all kinds. These modules can be combined in any number, but each weapon is locked individually. Individual removal is only possible after the entry of a unique PIN code or via fingerprint or contactless transponder activation.

But other systems are at a similar stage of development to these intelligent stationary systems. Safety systems that prevent unauthorized use are also already available and have been used successfully for years in securing inherited weapons in accordance with section 20, paragraphs 3–4 of the Weapons Act. In accordance with Figure 7 of the technical directive ‘Blocking Systems for Inherited Firearms’ (Germany, 2008), these safety systems have to withstand the attacks described in the directive for at least 30 minutes, thus requiring a significantly higher safety standard than gun safes with zero theft impediment. The National Metrology Institute of Germany carried out these tests and subsequently approved the system. Since it has been in use, the author is not aware of any incidents of misuse. The device was certified for use with a .55-calibre weapon. The same technology for locking weapons could also be used by normal gun owners.

What potential is there in a weapons-locking system such as this? If the gun is secured with a locking element, only its owner can unlock it; this can be done in less than two seconds. It can be released either with a PIN code or by using a biometric characteristic of the gun owner, or with both. Its critics make this seem difficult, but it is easy to handle and above all it is a tried-and-tested technology that is in widespread use in other identification systems. If the gun owner is travelling with the firearm and it is secured with a locking device, it can be stolen, but it is useless to the thief because he cannot use it. Current regulations require a secure transport container that can in fact be opened in a few seconds, but creates the illusion of security. Thus the protection factor is negligible, but the fiction is maintained. If the gun owner has secured his weapon with a gun lock, not only is he able to secure his weapon—for instance, while it is being transported—but, most importantly, he can also secure it in a gun safe of the kind that is so easy to open.
Perspectives

Obviously, all these issues affect important industry interests. The gun-safe-manufacturing industry has a keen interest in this market and it would be naïve to expect it not to let go of its erstwhile monopoly without a fight. However, the main concern is improving gun security in terms of unauthorized weapons use and the safety of our children. It will be sufficient if intelligent safety systems already on the market are licensed as alternatives to already certified existing systems, then the market will find its own level.

The next step is to work through the parliamentary initiative in a considered way and highlight the potential for introducing intelligent firearms-safety systems. An initial step could be the licensing of alternative intelligent systems and checking how marketable they are. The long-term objective is still to make the world safer and not to expose children—or anyone else—to the risk of being killed as the result of unauthorized or abusive possession of firearms. The firearms-safety systems already on the market are sufficient to ensure this, and it is high time that politicians and administrators made some progress in regulating their use. The legal context to do so has been provided by the 2009 amendment to the Weapons Act.

About the author

Jörg Schönbohm became an Army officer-cadet in 1957, took command of the East-German Armed Forces in October 1990, and concluded his military career in 1992 as Chief of the Army. He served as State-Secretary for 4 years, then as Senator of Interior of Berlin for 3 years. He then served 10 years in office first as Deputy Prime Minister then as Minister of Interior. Now retired, he lives in Kleinmachnow.

References


—. 2009b. ‘Reduction of Legal Firearms, Large-calibre Ban etc.’ Deutscher Bundestag Official Record 16/13473. Application of Die Grünen of 17 June:


Key Perspectives and Insights on Personalized Guns

Stephen P. Teret

Introduction

As the term is used in this paper, personalized guns are small arms (revolvers, pistols, rifles, and shotguns) that are designed and built to contain technology integrated into the gun itself that discriminates between authorized and unauthorized users, making the firing of the gun by an unauthorized user preventable. The technology to personalize guns presently exists, although the availability of such guns has not yet become widespread, largely for political reasons. Once they become widely manufactured and distributed, and begin to replace traditional guns that can be operated by anyone, the incidence of firearm-related morbidity and mortality will decrease. This paper will discuss the need for personalized guns, as well as the history, technology, public acceptance, politics, and law related to such guns. Emphasis will be placed on events, policies, and law within the United States because much, but not all of the activity regarding personalized guns has occurred there. In this paper the use of the term ‘personalized guns’ is synonymous with ‘smart guns’, ‘owner-authorized guns’, and ‘childproof guns’.

The need for personalized guns

The number of people killed worldwide each year by small arms is both difficult to assess and controversial. In its Global Burden of Armed Violence report, the Small Arms Survey estimated that ‘at least 526,000 people die violently every year’ (Geneva Declaration, 2011). Out of this global figure, between 42% and 60% are firearms related deaths (Geneva Declaration, 2008). Sceptics of this figure, such as the noted pro-gun advocate David Kopel, suggest that the number is smaller, but still in the hundreds of thousands (Kopel, Gallant, and Eisen, 2010). In a country for which accurate records are kept—the United States—total firearm deaths for 2010 were 30,672, with 61 per cent of those being suicides, 35 per cent homicides (excluding legal intervention), and the remainder either accidental or of undetermined intent (CDCP, 2013).

The number of these deaths that would be prevented by personalized guns is a function of several factors. Firstly, a large reservoir of existing firearms in civilian hands are functional and available for homicides, suicides, and unintended deaths. Secondly, some, but not all gun deaths are accomplished as a result of an authorized gun user pulling the trigger. Clearly, therefore, once personalized guns are introduced into the marketplace, some gun deaths will be averted, but not all of them. Critics of personalized guns point out that such guns will not address all gun deaths, but this argument would be true for any safety or health device. For example, antibiotics are not an effective method of preventing many chronic diseases, but we still embrace antibiotics for the lifesaving benefits they confer against many infectious diseases. Others argue that with so many handguns presently in homes, why bother making a safer gun? This would be
tantamount to arguing that because at one time there were so many automobiles without seatbelts or air bags, why make newly built automobiles with these safety devices? The answer is that we need continually to improve manufactured products by incorporating new safety technologies to reduce the unacceptable toll these products take on the public’s health.

The types of gun deaths and injuries that would be most affected by the advent of personalized guns are accidental gun deaths, youth suicides, and assaultive and homicidal shootings.

Unintended shootings that take place when a young child finds a handgun, though small in number compared to suicides and homicides, are particularly tragic and preventable. As discussed below, gun makers have been aware of these types of shootings for well over a century and now have the capacity to eliminate them, as well as other types of unintended shootings. Vernick et al. (2003) examined a series of unintended gun deaths in the states of Maryland and Wisconsin in the United States and estimated that 37 per cent of these deaths would have been avoided had the guns in question been personalized.

Youth (ages 0–19) suicides by gunfire, which in the United States represents 7 per cent of all firearm-related suicides (CDCP, 2013), are also preventable in that most youths would not be authorized to fire a personalized gun. Some sceptics might suggest that the absence of an operable gun would just cause a depressed teenager to find another means of suicide, but research shows that substitution or displacement of means of suicide frequently does not occur (Daigle, 2005). Also, the case fatality rate for intentionally self-inflicted gunshot wounds is much higher than for most other means of attempting suicide, i.e. there is little emergency medicine can do to save the life of someone who has shot him-/herself in the head compared to someone who has ingested pills.

With regard to criminal, assaultive behaviour with guns, an estimated 500,000 guns are stolen each year in home burglaries in the United States (Cook, Molliconi, and Cole, 1995), and these guns enter the illicit market. If such guns were inoperable by the thief or the persons to whom the thief sells the guns, gun crime resulting in deaths would decrease.

Some argue that the solution to the large number of gun deaths is to educate the gun-owning population and those who live with them (e.g. their children) to act carefully in the presence of guns. Such a reliance on safety training is misplaced. Understandably, children act like children, even after they have been instructed about the dangers of guns (Hardy, 2002). Even those who provide gun safety education are subject to error. Recently, in Maryland in the United States a police trainer in firearm safety accidentally shot a police cadet in the head (George, 2013).

The background and history of mechanical firearm personalization technology

In the 1880s D. B. Wesson, one of the founders of the prominent gun company Smith & Wesson, learned of a young child shooting another with a handgun. Wesson asked his son, Joseph, a gun designer, to create a childproof handgun to eliminate such incidents (Jinks, 1977). The result was a handgun that employed a grip safety on the rear of the gun that had to be squeezed at the same time that the trigger was pulled in order to fire the gun—a task that Smith & Wesson stated was beyond the ability of a child under the age of eight years (Teret and Culross, 2002).
The company sold more than a half million handguns utilizing this technology between 1886 and 1940 (Jinks, 1977). While this falls short of the personalization or modern childproofing of guns, it illustrates both the need for and the feasibility of changing the design of guns to prevent their unwanted discharge by young people.

A Smith & Wesson ‘Childproof’ revolver developed in the 1880s, showing the grip safety.

Other mechanical (non-electronic) ways of personalizing guns were used by some companies in the latter half of the 20th century. The Tri-C Corporation of Meriden, Connecticut sold the Fox carbine in the 1970s that utilized a three-wheel combination lock design to prevent unauthorized use. In its sales brochure the company marketed this device by stating ‘Accidental and unauthorized firing is prevented by a patented and built-in combination lock safety (which can easily be set by owner to any of 1000 possible combinations)’ (Fox Carbine, n.d.). In 1997 Taurus International, a manufacturer of revolvers, pistols, and rifles, introduced a lock-and-key device on its firearms that it stated in its advertising renders the firearm ‘inoperable at the turn of a key’ (Taurus International USA, 2013).

A Fox TAC-1 carbine, from the 1970s, utilizing a three-wheel combination lock
Early experiments to electronically personalize handguns

Undergraduate engineering students at the Johns Hopkins University produced a prototype of a personalized handgun in 1992. Faculty in the university’s School of Public Health gave the students a USD 2,000 grant and a disabled revolver and requested them to convert it into a gun that could be fired only by an authorized user. The students employed touch memory technology, which involved a small battery and a reader on the grip of the gun. A semiconductor chip in the possession of the authorized user that stored a unique serial number had to come in contact with the reader on the gun in order for a blocking mechanism built into the gun to move, allowing the gun to fire. Although patents issued to others had earlier proposed electronic ways of personalizing guns (US patent 4,467,545), this prototype was among the first to actually demonstrate the ability to inexpensively and readily place electronics in guns for safety purposes.

Sandia National Laboratories performed a comprehensive evaluation of other smart gun technologies for the US government in 1996. The report (Weiss, 1996) describes in detail what was available at the time using radio frequency identification, touch memory, and biometric (e.g. fingerprint reading) technologies. The report was commissioned to assess whether then currently available technologies could meet the special needs of law enforcement officers regarding user-authorized firearms. Its conclusion was that police officers have highly idealistic expectations regarding personalized weapons and that existing technology had not yet reached the level of perfection needed to meet their specialized demands.

In an effort to encourage the further research and development of personalized gun technology, the US government, through its National Institute of Justice, established a grant programme for interested gun makers. On 12 May 2000 President Clinton announced that two USD 300,000 grants were being awarded to Smith & Wesson and FN Manufacturing. A White House press release stated that

Today’s grants will support the design and testing of smart gun prototypes as well as additional research into specific technologies, including fingerprint identification and embedded microelectronics, to prevent firing by unauthorized users (White House, 2000).

Later in 2000 the US Congress appropriated considerably more funds for such research and development, which were granted by the National Institute of Justice to both gun manufacturers and electronics firms.

In about 2002 a subsidiary of the Mossberg Technology Group, iGun Technology, developed a personalized long-gun, which it describes as follows:

The ITC iGun™ works on mechanisms that block the trigger while the gun is at rest. The user wears a ring with a special system that triggers power to the iGun system when the ring comes in close range to the normal ring-finger placement on the firearm’s stock. When the iGun senses that the ring is near enough, it compares a unique code (billions of combinations) from the ring to the gun to see if there is a match. If the code matches and certain other conditions are met, an electric current from the battery bank actuates a mechanism to unblock the trigger (iGun Technology, n.d.).
US legislative and litigative activity

In the absence of meaningful voluntary efforts by most established gun manufacturers to incorporate personalization technology into their products, exploration was begun in the United States of strategies for mandating guns to be personalized through legislation, regulation, and litigation.

In 1997 the attorney general of Massachusetts, Scott Harshbarger, promulgated regulations designed to make new handguns sold in that state childproof (Massachusetts, 1997). But the regulations, some of which were later adopted by the state legislature into statutory law, did not require personalization technology: indeed, technology such as the Smith & Wesson childproof handgun from the late 1800s might have satisfied the childproofing portion of the Massachusetts law. Similarly, in 1999 California passed a law requiring firearms sold in the state to be accompanied by a state-approved safety device designed to reduce the likelihood that a child could discharge the weapon, but personalization was not mandated (California, 1999).

The first suggestion for legislation mandating personalization came from the Johns Hopkins University’s Center for Gun Policy and Research, which in 1998 published A Model Handgun Safety Standard Act (DeFrancesco et al., 1998). This offered a blueprint for states and localities in the United States to establish, through a commission, a performance standard for all newly manufactured handguns sold in that jurisdiction. The standard would require built-in personalization technology that could not be readily deactivated.

Based on the Johns Hopkins model law, in 2002 the state of New Jersey enacted a law providing that once a personalized gun is introduced for sale in the state and is recognized by the New Jersey attorney general as complying with the statutory definition of a personalized or childproof gun, then three years after that date all new handguns sold in the state must be personalized (New Jersey, 2002).

Bills have been introduced in the US Congress calling for a mandate that some guns be personalized or childproof, but these bills have not been enacted into law. For example, in June 1999 Congressman Pascrell and others introduced HR 2025, which called for a ban on the manufacture of handguns that are not personalized. Other members of Congress are currently considering introducing similar bills.

Most recently, a bill has been introduced into the Californian Senate that would require that 18 months following the state attorney general’s reporting that owner-authorized (i.e. personalized) handguns are available for retail sale, all handguns sold in California would have to be owner-authorized (California, 2013).

Given how difficult it is to pass legislation mandating personalized guns, it had been thought and suggested that litigation could force gun makers to utilize personalization technologies. The scenario was posed that a person injured or killed by another with a gun that the shooter was not authorized to operate could sue the gun maker for its failure to make an adequately safe product (Teret and Culross, 2002). The use of litigation to enhance the safety of cars had been successful and it seemed that the same strategy could apply to guns (Teret, 1986). But in 2005 the US Congress passed the Protection of Lawful Commerce in Arms Act, which provides extensive immunity to gun makers from many product liability lawsuits (Vernick, Rutkow, and Salmon, 2007).
**Current technical options for personalizing guns**

Recent developments in technology now permit the manufacture and sale of personalized guns. The most promising technologies involve radio frequency identification (RFID) and biometric recognition devices.

RFID utilizes ‘tags’, which can be objects containing tiny electromagnetic transmitters, and ‘readers’, which receive the information from the tags. RFID is now widely in use, allowing for controlled building access, vehicle parking access, and library book theft prevention, among many other uses (Roberts, 2006). With regard to guns, RFID enables a gun maker to provide a tag in a wristwatch, ring, bracelet, or other device that communicates with the reader embedded in the gun (often in the grip of a handgun). When the reader detects the tag, a mechanical device in the gun can move a blocking mechanism that has been preventing the firing of the gun, thereby allowing it to be fired. Without the tag being in close proximity to the reader on the gun (i.e. when the gun is being held by an unauthorized user), the blocking mechanism will remain in place, rendering the gun inoperable.

TriggerSmart™, an Irish company, is an example of a start-up business that has recently developed RFID technology for use in a personalized pistol (TriggerSmart Technologies, 2013). The TriggerSmart™ high-frequency RFID system establishes communication between the firearm and a bracelet in order to authenticate a user. The firearm’s battery, antenna, and electronic interface are built into the handgrip of the gun. Once the radio frequency tags in the bracelet fall within a distance where it can communicate with the antenna in the handgrip, the gun enters an ‘instant on’ phase where it can be fired.

Armatix, a German company, has produced the iP1 pistol, which is a personalized .22 calibre handgun that works like a conventional pistol, except for the fact that it is digital and battery operated, which allows for software flexibility, depending on the needs of the consumer (Armatix, 2013). The Armatix pistol is accompanied by an RFID wristwatch (designated by Armatix as iW1) that uses radio frequencies to activate the handgun, making it operable. The watch also uses a personal identification number (PIN) that must be entered in order to unlock the electromechanical firing pin lock, making the gun operable by the owner (Armatix, 2013). Armatix is interested in licensing other gun makers to use its technology.

Kodiak Industries (which also refers to itself as Kodiak Arms) in Salt Lake City, Utah, debuted a retrofit personalization product for existing pistols at the Shot Show in January 2013. This product, which the company says it is ready to mass market, replaces the grip on an ordinary pistol, and the new grip reads the fingerprint of the person holding the gun. The fingerprint-reading computer chips will be designed to recognize the prints of up to 20 different people (Kodiak Industries, 2013).

Another company working on fingerprint reading is Safe Gun Technology, which describes its product as follows:

> The key differentiator of the SGTi™ technology is that every element of user-authorized small arms safety technology is fully incorporated in the small arm itself, and no external device or component is required for operation thereof. Unlike the wrist watch concept or the ring concept, SGTi™ technology cannot get lost or otherwise separated from the firearm. Further, unlike systems that require repetition or ‘training’ of the
firearm to recognize a user, SGTi™’s user-friendly technology allows a master user to easily and rapidly add or delete additional users (Safe Gun Technology, 2013).

The New Jersey Institute of Technology has been working for years on a different form of biometric recognition in a personalized gun. Its product employs ‘grip recognition’. The handgun, after some period of use by its owner, recognizes the palm configuration of the owner and will work only when held by this authorized user.

Current perspectives

While the technology for firearm personalization has progressed impressively over the past two decades, now allowing for the production and distribution of such guns, controversy still surrounds making changes in guns as a consumer product. Some lingering questions remain regarding certain aspects of the technology, and the politics of personalized guns are being fought hard.

As to technology, some are proponents of RFID personalization and others favour biometrics. But there is no need for governments to choose one technology over others. Competition among gun manufacturers with regard to competing technologies is helpful and ultimately the purchasers of such guns will determine whether one technology is favoured. If governments want to regulate the safety of guns, as they have regulated the safety of other consumer products, they can do so by the promulgation of performance standards that mandate issues such as reliability, leaving to the manufacturers how they achieve such reliability, rather than setting design standards.

The factor that influences the widespread availability of personalized guns is currently politics more than technology. In January 1999 Beretta issued the following statement regarding smart guns:

As the leading designer and manufacturer of high-quality firearms in the world, Beretta has recently been asked by several news organizations about the feasibility and advisability of making handguns that include so-called ‘smart gun’ technology or ‘personalized’ internal locks. Beretta has considered this issue for several years and has concluded that existing design concepts of this type are neither advisable nor feasible.

Although the concept of a ‘smart gun’ or ‘personalized gun’ has received public attention recently, we believe that careful consideration has not been given to potentially dangerous risks associated with these concepts. In our opinion, such technology is undeveloped and unproven. In addition, Beretta strongly believes that ‘smart gun’ technology or ‘personalized’ guns ... could actually increase the number of fatal accidents involving handguns (Beretta, 1999).

The public position of most (but not all) gun makers has not changed substantially in the past decade or more. Unlike the manufacturers of other products, who have embraced technology to make their goods safer and more attractive to the public, gun makers still rely on designs that are a century old. The National Shooting Sports Foundation in the United States, which is the trade association for the gun industry, still claims on its website that personalized guns are ill advised, citing the 1996 Sandia report that focused on police weapons:
‘Personalized’ or ‘smart gun’ technology, while in development stages, is neither reliable nor available. A U.S. Dept. of Justice-funded project, researched by Sandia National Laboratories, concluded, ‘There is not currently a perfect smart gun technology.’ Owner-recognition technology, such as fingerprint recognition or a radio transmitter, requires a power source to work. Any technology that relies on a power source will fail, possibly at the worst time imaginable (NSSF, 2013).

The fear that traditional gun makers express about personalized guns appears to stem from two situations. The first is the threat of punishment from gun groups if the manufacturer embraces new technology and the second the fear that governments will mandate that all new guns be made personalized, which would make the manufacturers’ present product lines obsolete, resulting in a loss of revenue.

This fear from gun groups is not just based on conjecture, but comes from the memory of the devastating boycott that Smith & Wesson faced a few years ago. At the turn of the 21st century gun makers, including Smith & Wesson, were being sued by local and state governments, as well as the US federal government. The bases of these lawsuits were that the manufacturers allegedly were not taking adequate care in their distribution systems to keep guns out of the hands of criminals, nor were they designing their guns as safely as was feasible. In an effort to settle the lawsuits against it, Smith & Wesson agreed to make changes in both its distribution system and the design of its guns. In doing so, it broke rank with the other gun makers and with groups such as the National Rifle Association. The punishment levelled against Smith & Wesson was swift and severe. Boycotts of its products were begun and the company had to close its factory temporarily due to severe declines in revenue.
There are concerns that legislative mandates for the personalization of new guns, such as that passed in New Jersey in 2002, would cause financial hardship for some makers of traditional guns that refuse to utilize new technologies. But governments have a well-established duty to protect the health and safety of the public, and a gun manufacturer that refuses to make use of safety technology should have no cause to complain about financial loss any more than a car maker would about financial loss for its failure to use seatbelts and air bags.

After the tragic shooting deaths of 20 young children in Newtown, Connecticut, President Barack Obama established a Task Force to explore many methods to reduce the incidence of gun violence in America. One of the meetings of the Task Force, in January 2013, focused on technology, and the subject of personalized guns was prominently featured. When Obama declared 23 executive orders shortly thereafter, one of them called for the US Department of Justice to more fully explore the benefits that personalized guns offer. A report from the National Institute of Justice is forthcoming.

Meanwhile, venture capitalists in the United States have become interested in investing in the further development of personalized gun technology (Henderson, 2013).

The widespread availability of personalized guns seems to be inevitable: the technology is currently available and will soon be enhanced; the political will to foster its availability appears to be present at national and local levels; and the interest of the media and the public is growing. After decades of delay, this lifesaving technology is finally coming to fruition.

About the author

Stephen Teret is a Professor at the Johns Hopkins Bloomberg School of Public Health in the USA. He directs the School’s Center for Law and the Public’s Health, and is the Founding Director of the Center for Gun Policy and Research. Professor Teret is also a faculty member of the Johns Hopkins School of Medicine. Trained as a lawyer, Teret spent ten years as a litigator in New York before earning his degree in public health and joining the faculty of Johns Hopkins University. Professor Teret has served as a consultant to all levels of government in the United States, including consulting to the President and the Attorney General of the United States.

References

Armatix. 2013. ‘Armatix iP1 Pistol.’ <http://www.armatix.de/iP1-Pistol.779.0.html?&L=1>


California. 1999. California Penal Code, ss. 12087.6, 12088–12088.9, and 12126.


New Jersey. 2002. *New Jersey Statutes,* Title: 2C, ch. 58, ss. 2C:58−2.2 ff.


Using Computer Technology to Increase Gun Safety

Michael Recce

Introduction

Computer technology is rapidly changing the way people live. In particular, small, inexpensive computing devices are embedded in everything from our cell phones to our washing machines and cars. Automotive safety, access security, and security in commerce all now depend on small embedded computing devices. This survey looks at ways in which these same computing devices can be used to increase gun safety and security.

Firearm-related deaths in the United States are eight times higher than countries with a comparable level of economic development (Krug, Powell, and Dahlberg, 1998). Also, firearm-related deaths of children aged 14 and under are 25 times higher in the United States than comparable high-income countries (CDCP, 1997). National opinion surveys in the United States have clearly shown that the majority of the population wants a reduction in gun-related accidents and deaths (Smith, 2001). However, the same surveys show that the population is not interested in banning access to guns, just in decreasing the unacceptable incidents and accidents that occur with these guns. This can be achieved through legislation, technology, or other means. This paper critically examines ways in which technology can help. In particular, it evaluates technology that restricts the use of a gun to authorized users, i.e. personalizes gun usage.

Before examining solutions, it is important to understand the scope of the problem. The first section of the paper looks at ways of classifying types of gun-related incidents, e.g. unintentional shootings, suicides, homicides, and other gun-related crimes. A technology that reduces one type of incident may not help in another. This classification makes it possible to separately discuss and evaluate the impact a specific technology can have on each type of incident.

The second section reviews a range of technological ideas that have been or are being developed to personalize guns. It begins with a description of common characteristics of these solutions. In particular, it only discusses technological approaches that involve a computer chip and battery. Many non-computer-related technologies, like trigger locks and gun safes, restrict gun access to authorized users. The focus here is on the safety and security issues that occur after a lock has been removed or a gun has been removed from a safe. Each personalization technology is described, the way in which it could impact the various types of gun-related incidents is discussed, and related risks and concerns are analysed.

The paper also describes in some detail the DGR biometric gun that was developed by the author and his colleagues at the New Jersey Institute of Technology (NJIT) (US patent 6,563,940).

The final section of the paper presents a perspective on ways in which this technology may gradually be integrated into guns.
Background: defining the problem

Gun violence is a regularly debated political issue and the extent of the gun-related problem in the United States is clear, creating possibilities for personalized technology to mitigate this problem.

According to the National Center for Injury Prevention and Control, in 2000 there were 52,447 deliberate and 23,237 accidental, non-fatal gunshot injuries in the United States (NCICP, 2000). There are on average five non-fatal firearm injuries for every two deaths (Firearm and Injury Center, 2011). Most of these accidental shootings involved handguns in homes. A technology that increases safety might, for example, reduce the chances that the gun is inadvertently fired when it is being handled, but where there is no intention for it to be fired.

Nearly two-thirds of gun-related deaths are suicides, leading to questions about the possible impact of personalization technology. In some of these cases the shooters are not authorized users of the guns. The issue then becomes a measure of incremental benefit. How much does a problem have to be reduced by a technology for the incremental benefit to be worth the costs?

Each year there are numerous workplace, school, or public area mass shootings of innocent victims. In some of these cases the shooters are the registered owner of the guns and in other cases they are not. Again, can sufficient incremental benefit be gained from the technology?

According to Federal Bureau of Investigation statistics, dozens of law enforcement officers in the United States are killed each year by criminals who take away their guns (FBI, 2012). In over 40 per cent of these incidents the officers are shot with their own guns.

According to the US Department of Justice (Langton, 2012), on average, 232,400 firearms are stolen from private citizens each year. Most personalized guns would not be usable if they are stolen. Personalization can also limit the ability for convicted felons to use intermediaries to purchase guns for them.

Methods to personalize gun usage can positively affect each of these facets of the problem. One published report estimates that a personalized gun could have prevented 37 per cent of handgun-related deaths (Vernick et al., 2003). In the recent briefing from the Task Force that evaluated gun safety options, Vice President Biden said: ‘a lot could change if, for example, every gun purchased could only be fired by the person who purchased it’ (LoGiurato, 2013).

However, the magnitude of any attempt to introduce personalized technology is also clear. According to the National Institute of Justice, in 2009 there were 310 million guns in American households (ATF, 2011, p. 15). A Gallup poll in 2004 indicated that 49 per cent of men and 33 per cent of women in the United States said they owned a gun. With this many guns already in households, an important question is how technology to personalize gun access can be added to existing guns.

Technology to personalize guns

In order to measure the potential impact of personalized gun technology, it is important to understand how this technology works.
Ideas for building personalized guns have several common elements. All of these systems have to have a way for the shooters to prove they are authorized to use the gun, like having the key to a lock. The ‘key’ in these systems is detected by an electronic sensor that measures something for verification. In some designs this sensor measures something about the authorized user, called a biometric. In other designs it measures something that the authorized user has that acts like an electronic key.

There are two major types of biometrics: physical biometrics and behavioural biometrics. A physical biometric is a unique observable property of an individual, like for example his fingerprints, DNA, iris patterns, or facial features. In contrast, a behavioural biometric is a unique property of an individual’s behaviour, like how he/she signs her name or the characteristics of his/her voice.

An alternative to a biometric is to use the sensor (key) to detect a combination code typed into a keypad or an electronic signal for a separate key device, like using a push-button lock to unlock a car. The technology used in near-production prototype guns is radio-frequency identification (RFID). The same technology is commonly used on toll roads in the United States to identify your car and pay your fee. In personalized guns that use RFID the shooter wears a ring or wristwatch that emits the ‘key’ signal that unlocks the gun.

In all of these designs a computer chip in the handgun recognizes a signal (the key) and allows the gun to fire (undoes the lock). The lock itself is usually an electromechanical device that moves inside the gun and unlocks it when the shooter is authorized. Electronically fired ammunition is also being developed that would remove the need to mechanically disable the gun (US Patent 5,625,972). With this ammunition the bullet is fired using an electronic signal from the computer. Handguns that use this technology are still a few years away.

All of these designs for personalized guns require batteries to power the electronics and sensors. In many respects the electronic components added to personalize a handgun are similar in complexity and cost to the components of a simple cell phone. This technology, like that in cell phones, is mature and sufficiently inexpensive to allow a type of cell phone that is commonly referred to as disposable.

Since the mid-1990s many different personalized guns have been constructed and are becoming commercially available. Kodiak Industries has a gun called the Intelligun that uses a fingerprint reader on the handle as a key and has an alternate key system to override the biometric. According to the website http://www.intelligun.com, this handgun is commercially available.

Armatix produces a range of gun-locking systems and a handgun that is activated by an RFID-authenticating signal in a wristwatch or ring (http://www.armatix.de). An RFID-activated handgun has also been developed by Trigger Smart (http://www.triggersmart.com).

The author and colleagues at the NJIT developed a range of prototype handguns using a behavioural biometric called Dynamic Grip Recognition (DGR). When the trigger of a gun is pulled the shooter’s hand applies a pressure pattern to the grip of the gun that is based on his/her bone structure, hand size, and behaviour patterns. This grip pattern differs from individual to individual in much the same way as a signature does. The grip dynamics are captured by pressure sensors around the handle (piezoelectrics) that are similar to pressure sensors on the touch pad of a laptop computer.
The author (left), with New Jersey Governor James E. McGreevey, demonstrating a smart gun utilizing Dynamic Grip Recognition technology, Newark, January 2004. Photo: Mike Derer / AP Photo.

Risks, limitations, and concerns

A wide range of concerns have been raised with respect to embedded technology in handguns (Friess, 2002). In this section these concerns are evaluated, along with potential methods for addressing them. Some of the concerns apply to all of the methods for personalizing weapons and others are specific to a particular method.

Perhaps the top of the list of general concerns is battery failure or loss of power, and of particular concern is the possibility that the battery fails and the gun is left locked. Apart from the battery, there is a concern that the electronics may not survive in the hostile environment within a handgun, where there are explosions and rapid changes in temperature. A third concern with adding digital electronics to a handgun is the impact that the additional components have on the cost of the gun. Also, there is a concern that the technology will make guns more difficult to use or will slow down a shooter who needs to fire the gun quickly (e.g. in self-defence).

There are many methods for reducing the risk of battery failure. In particular, the gun can be designed to switch on if the computer chip detects that the battery is about to fail (Recce, patent under review). Battery technology is being driven by the market growth in hand-held
computing devices. The reliability and power storage properties of batteries are continuing to improve. Furthermore, as in the NJIT prototype, the battery can be in the magazine and charged like the battery pack of a cordless drill. In the NJIT prototype the battery is only used when the trigger is pulled, otherwise the system uses little power, resulting in a long battery life.

In many of these gun designs the electronics are in the handle of the gun, far away from the chamber or barrel where significant mechanical vibration and temperature changes occur. The electronic components are very inexpensive, similar to those in inexpensive cell phones. Growth in the personalized electronics industry is continuing to reduce the cost and power consumption, and to increase the reliability of these components. The components can perform tens of millions of computations in the fraction of a second it takes to pull the trigger, so they do not slow down the firing of the handgun.

Separate potential failure modes have been identified for each of the different designs for personalized handguns. With the designs that use a secondary device, like a ring or wristwatch, to provide an authorizing RFID signal the gun owner has to remember to wear the secondary device in order to shoot the gun. If the secondary device is kept together with the gun then limited additional security is provided by the ‘key’ mechanism and an unauthorized user who has access to the secondary activating device could use the gun. An additional concern with using a secondary activating device is that it may be possible to use electromagnetic interference to block the communication between the authorizing device and the gun, and therefore to render the gun inoperable.

One of the concerns with the biometric handgun prototypes is reliability. Stated simply, can the sensor really identify the shooter? There is also a concern that these guns could not be shared by a set of authorized users. The prototype that uses fingerprint recognition could not be used with gloves, unless the authentication was inactivated, but sceptics more readily accept that fingerprint readers work. Dynamic grip recognition is harder for some to accept, but it works with gloves and uses less expensive sensors. Also, there is a concern that in a high-stress state, when the gun is really needed, an individual’s grip pattern is different, making the gun inoperable at a critical time. A non-technological concern with biometrics is that they imply a decrease in gun freedom. In particular, the gun would require a registration process where the biometric would be measured and recorded in the gun, making it more difficult to give or sell it to a neighbour.

The top two technology concerns with DGR are that a grip may not be unique and that the system may fail to recognize the owner’s grip at a critical high-stress moment. The failure to block an unauthorized user of the gun is called a false positive and the failure to allow the legitimate user is called a false negative. As in most statistical decisions, it is possible to make a trade-off between these two types of errors. In particular, the NJIT prototype is set to have a false negative rate (failure to allow the authorized user) that is lower than the mechanical failure rate of the gun and a false positive rate of 10 per cent. This means that one in ten unauthorized users would be able to use the gun. The grip recognition technology in the NJIT gun has also been tested using a FATS simulator (Meggitt Training Systems). The FATS simulator, which is used for training police officers, uses virtual reality to simulate high-stress scenarios.

The computer chip and memory in both types of biometric gun can store the authorization patterns or fingerprints of many users. So the gun would not be restricted to use by only one individual or only one hand.
Inside the DGR prototype

The handgun used in the NJIT DGR prototypes has undergone several modifications, as shown in Figure 1. The grip plates on either side of the gun have been replaced by two computer boards that have pressure sensors on the outside and electronic components on the inside. A hole that contains the disabling device has been drilled above the trigger and below the barrel. A hole has been milled out of the trigger to allow a magnet to be embedded and a sensor to detect this magnet has been put into the trigger guard.

When the trigger is pulled the magnet (6) moves past the sensor (7), turning on the computer chip. The chip reads the pressure sensors on the outside of the two computer boards (shown in Figure 2).
If the shooter is recognized, a green light is lit on the back of the gun, the disabling mechanism is activated, and the gun fires a round. If the user is not authorized, a red light is lit on the back of the gun and the disabling mechanism remains in place, stopping the gun from firing.
Reducing incidents and accidents with personalized guns

In the debates about the use of technology in guns the key question is how to make the trade-off between the incremental benefit and costs. How great an increase in gun safety or security is needed before personalized guns are actively sought by law enforcement officers or in private households? How much impact do they have to have on the categories of gun problems outlined above before they are legally mandated? What impact could this type of technology have if there are already so many guns in households?

All of these technologies would reduce unintentional gun accidents. The RFID-enabled guns can only be fired if the secondary enabling device is nearby, which will most likely not be the case during cleaning and handling, or if a gun is dropped. Both types of biometric guns (i.e. with fingerprint or grip recognition) require the hand to be on the grip and the finger to be on the trigger in order to fire the gun. In all four cases the gun is much less likely to be accidentally fired and therefore the number of incidents of accidental harm should decrease.

The unauthorized use of guns in homes would also decrease with either RFID or biometric technology in guns. As discussed above, the decrease in unauthorized use would probably be greater with biometric technology, since many private residents may leave the ring or watch that authorizes the gun near the gun.

Including computer technology does not solve the problem in any of the identified areas, but it does provide incremental benefits. Most new medicines merely provide incremental benefit, but they are put into use. Childproof caps on medicine bottles and airbags in automobiles are also examples of developments that provide incremental benefits. The same principle applies to the use of personalization technology for guns. The technology used in personalized guns will also continually improve as commercialization progresses.

Future directions in personalized guns

In mid-March 2013 a group called the Sandy Hook Promise Innovation Initiative was started in San Francisco (Nocera, 2013). This group plans to provide start-up funding for companies that are focused on applying technology to increase gun safety. This initiative, which is taking place in the heart of the computer industry, along with other initiatives, should continue to spur innovation. Technology can help increase gun safety and security, and the right marketing, innovation, and perhaps legislation will bring handguns into the computer era.

Once computers are in guns we can expect the other types of information to be available that technology provides us with in our smart phones. For example, when a gun is fired, it will be possible to store the exact time, the exact place using the GPS system, who fired it using the biometric sensor, and even the direction it was pointed in. The advantages of this to law enforcement are obvious.
About the author

Michael Recce is an Associate Professor of Information Systems at the New Jersey Institute of Technology, and was previously a lecturer at University College London (Neuroscience and Computer Science). He received a BS in Physics from the University of California Santa Cruz and his doctorate in Neuroscience from University College London. Michael has six patents, including two for a biometric called dynamic grip recognition. For seven years, Michael worked extensively with financial institutions devising improved methods for detecting money laundering and terrorist activity in financial transaction data. Early in his career, Michael was a product engineering manager at Intel Corporation.

References


