BACKGROUND
All around the country, states and municipalities are rushing to install public surveillance cameras in an expensive and misguided attempt to fight crime. Unfortunately, studies show that these cameras do not prevent or help to solve most crimes. To make matters worse, they are expensive, commonly misused and intrude on our constitutional rights.

PROPOSALS

• **Study** of the effectiveness of surveillance cameras in preventing and solving crimes compared to other measures, along with a full analysis of the actual costs of camera systems to governmental entities in Texas.

• **Increase** accountability by requiring governmental entities to consider alternative policing measures and draft a comparison report, including a calculation of the ongoing costs to be borne by the entity, before installing cameras in public places.

• **Require** governmental entities currently using public surveillance cameras for policing to publicly issue a quarterly report with a full accounting of all surveillance-related costs.

• **Amend** state open records laws to narrow the surveillance camera exceptions in Texas Government Code section 418.182.

EXPLANATION

Cameras Are Ineffective at Stopping Crime
Studies of the following cities show that installing surveillance cameras did not result in a meaningful reduction in crime:

• Los Angeles
• San Francisco
• London
• Glasgow
The fact that public surveillance cameras are not effective at preventing and solving most crimes is surprising to some people, but there are many common-sense explanations for this fact. First and foremost, cameras do not deter most criminals, even violent ones. A camera cannot arrest them, and it may not even be recording. Second, many of those who are deterred simply move to another area that does not have video surveillance to commit crimes. Third, a camera must be operated properly to be effective, which is often not the case. For example, the University of Texas has a security camera focused on a statue of Martin Luther King, Jr. on campus. When the statue was egged in 2003, the recording device was not working and the university never caught the vandals.

Cameras Are Costly to Municipalities

Given the increase in federal funding for surveillance cameras in recent years, many municipalities see more cameras as a cost effective way to fight crime. These federal grants typically cover only the up front costs, though. There are many ongoing costs to video surveillance that end up falling to municipalities, including maintenance, upgrades, manpower and training. Perhaps the largest cost of all is the opportunities that are lost to put scarce resources toward more effective measures like improved lighting, community policing and foot patrols, instead of an ineffective surveillance system.

Camera Operators Are Often Unaccountable

An ACLU study of video surveillance in California found that of the 37 police departments that were using video surveillance, only 11 provided any written policies specifically addressing video surveillance. At the University of Texas, the Daily Texan quoted UTPD Chief Jeffrey Van Slyke saying “I don’t know where the cameras are.” UTPD monitors only a select few of the cameras on campus, leaving the installation to Information Technology Services. But ITS has no guidelines regarding who monitors the cameras and for what purpose. The Daily Texan also quoted William Stephens, an ITS systems engineer: “My concern is there’s no real policy on how these [systems] are managed. The University should have a policy.” In response to an open records request from the Daily Texan, the University of Texas lobbied successfully to exclude specifications, operational procedures or locations of public surveillance cameras from disclosure under state open records law. The Texas Department of Public Safety recently argued in court that this provision applies to video taken by these cameras as well.

“Billions of pounds have been spent on [cameras], but no thought has gone into how the police are going to use the images. It’s been an utter fiasco.”

– Detective Chief Inspector Mick Neville, London Metropolitan Police Force
Surveillance Camera Footage is Too Often Abused

Perhaps as a result of lax operational guidelines, law enforcement personnel have made serious, high profile abuse of surveillance cameras. Just days before the 2004 Republican National Convention in New York City, NYPD officers were using a helicopter equipped with an infrared camera to monitor a protest. This device is able to detect heat, which allows the police to see in total darkness. As the police surveyed the area, they focused on a couple who were kissing and fondling each other on a rooftop. After leaving the couple, the camera came back to focus on them repeatedly, recording extensive footage. That same year, surveillance camera footage of a young man who fatally shot himself in the lobby of a New York City public housing project surfaced on a pornographic website. In 2005, a San Francisco police officer who had been on the force for 25 years was suspended for using a surveillance camera at San Francisco International Airport to ogle women. Far from being the exception, these sorts of abuses are all too typical of public surveillance systems.

Cameras Are Invasive

Public video surveillance infringes on our constitutional rights in several ways. They have a chilling effect on the freedom of speech, association and movement by causing people to censor themselves out of fear that the government is watching. The Supreme Court has ruled that the First Amendment protects anonymity in public, particularly when citizens engage in political speech. This protection is seriously jeopardized when public places are under surveillance, particularly if the cameras being used are equipped with facial recognition software. In addition, the Fourth Amendment guarantees our right to privacy through freedom from unreasonable searches and seizures. This right is an individual one, and still applies when we are out in public. Modern video systems do not just record information that is readily observable. Using automatic identification and face and eye scans, they can collect and store information for uses that were never possible before. As technology advances, we need to make sure that free speech and privacy rights keep pace.

CONCLUSION

Texans are rightfully concerned about government installation of this invasive new technology without forethought or public input. Legislators should further study the effectiveness of public surveillance cameras in comparison to alternative policing methods to determine whether these systems are necessary.

RESOURCES


BACKGROUND

Governments and businesses are increasingly using biometric identifiers, in particular fingerprint recognition technology, for identification and security purposes. The Dallas Independent School District now has a fingerprint check-in system for hourly employees, administered by a private vendor. Many companies are beginning to use this technology instead of timecards. Microsoft currently sells a fingerprint reader, which allows computer users to sign into password-protected websites using their fingerprint. **As employers and private entities use fingerprints for identification more often, Texans are exposed to increased risks to their privacy, including identity theft.**

In 2003, the Texas Legislature passed a law regarding the capture, storage and disclosure of biometric identifiers for a commercial purpose, including fingerprints. This legislation was a step in the right direction. Unfortunately, it fell short in a few areas because it lacked a requirement for timely purging of biometric identifier records and does not sufficiently safeguard against biometric identifiers being sold to or shared with other entities.

PROPOSALS

- **Require** the entities who hold this data to destroy it within a reasonable time—no longer than one year after the purpose for collecting the identifier has expired.
- **Narrow** the circumstances under which a private entity can sell or share an individual’s biometric information, including a requirement that law enforcement officers obtain a warrant to gain access to biometric data.

EXPLANATION

Identity Theft

The use of biometric identifiers for commercial purposes creates serious privacy concerns. Identity theft is a growing problem in the Internet age, and there have been several high profile cases of identity theft in recent years. In February 2005, identity thieves raided a database of bank account, credit card and Social Security numbers operated by the company ChoicePoint, exposing as many as 100,000 consumers to identity theft. The Microsoft Fingerprint Reader was shown by a Finnish researcher to be vulnerable to hackers. In June 2008, a database
containing the driver’s license and Social Security numbers of 826 Texas state employees was stolen from L 1 Identity Solutions. Although no fingerprint data was stolen, many of these employees were waiting to be fingerprinted pursuant to a new law that was passed during the 2007 legislative session.

High Cost to Society
The costs of identity theft are already extremely high. A 2003 report paid for by the Federal Trade Commission estimated that 3.25 million Americans had their personal information misused to commit fraud in 2002, and this figure does not even include theft and misuse of credit card numbers. The total estimated cost of this fraud was $33 billion. As the use of biometric identifiers becomes more prevalent, there is potential for a great increase in the costs of identity theft. Identity theft costs individuals hundreds of hours of work to restore the integrity of their personal information.

Biometric Data is Permanent
The consequences of having your biometric data stolen go far beyond the hassle and costs of combating more traditional forms of identity theft. The government can change a driver’s license or even a Social Security number. Once your biometric data has been stolen, however, there is no remedy, because fingerprints, retinal scans and voiceprints can never be altered.

Protect Privacy Rights
Consenting to have your fingerprints collected so you can get a job is not the same thing as consenting to having your fingerprints collected for a law enforcement purpose. Texans who provide biometric data to their employer, bank or another entity should have the same Fourth Amendment protections we all cherish. They should be able to withhold consent to share their fingerprints with the government, unless law enforcement has a warrant for the information. Similarly, Texans should be protected from the unregulated sale or transfer of their biometric data between private entities.

CONCLUSION
As the uses of new biometric technologies expand, Texas law needs to keep up to ensure that all Texans are protected from new exposure to identity theft. Over time, digital copies of a person’s fingerprints in the wrong hands could undermine their value even as a law enforcement tool. To protect our privacy and public safety, biometric identifiers need better protections under Texas law.

RESOURCES
Electronics Privacy Information Center: http://epic.org/privacy/biometrics/default.html
BACKGROUND

Digital technologies used by business and government are a potential threat to personal privacy and security. Radio Frequency Identification (RFID) is a promising but little-understood technology. RFID is an automatic identification system that uses computer chips with antennas to transmit information about people or goods. When processed by a reader, an RFID chip can provide location or identification information that can be copied and stored.

You may already have an RFID chip in a credit card or passport and not even know it. With the right technology, your personal information can be read at distances ranging from several to hundreds of feet.

This leaves Texans open to identity theft or worse through a practice called “skimming,” the unauthorized reading of personal information stored in an RFID chip. Skimming is possible because many RFID chips have inadequate protections against hackers.

Skimmed information can be stored, cloned and used for identity theft and surveillance. Technology to skim personal information off RFID chips is already on the market, relatively affordable and easy to find. The Cato Institute reports that “we have yet to see an RF human identification system that does not collect and store information about every American subject to it for at least 75 years.”

Texans are rightly concerned about identity theft, invasion of privacy and government surveillance. Policymakers should not allow further implementation of RFID before investigating how to better protect the safety and identity of all Texans.

PROPOSALS

- **Halt** the use of RFID in schools and initiate a study on safety risks of RFID in the school environment.

- **Prevent** identity theft by imposing tighter security measures and limiting access to personal information.

- **Publicize** the location of RFID readers in an “RFID Right to Know Act,” making individuals aware of how their personal information is used and when and where it might be intercepted.

- **Conduct** a broad study on the effects of RFID to evaluate safety risks and potential for identity theft.
EXPLANATION

Texas is grappling with privacy and other issues as it moves closer to the use of enhanced driver licenses (EDL). EDLs are driver licenses that contain an RFID chip to speed border crossing, and can be used to prove identity and citizenship.

“RFID technology may have a small benefit in terms of speeding identification processes, but it is no more resistant to forgery or tampering than any other digital technology.”

– Department of Homeland Security

EDL is currently an unfunded program. Policymakers should insist that implementation of RFID technology include security protection such as limiting access to personal information and the length of time personal information can be stored before considering funding the implementation of EDL.

Despite widespread criticism, RFID is quickly gaining ground on the market. Security measures, however, are not keeping pace. RFID codes have been cracked in a number of supposedly secure settings, from British e-Passports to RFID-embedded credit cards. The benefits of RFID are not worth the risks.

Electronic Surveillance of Students

If RFID invites the invasion of privacy and identity theft, why is it being considered for tracking school children? RFID has been used in schools to streamline attendance-taking procedures or, as in Spring, Texas, in pilot programs to assess the effectiveness of RFID technology to establish student presence on school buses and inside school buildings. Further investigation is needed to fully assess if any small benefits are worth the invasion of privacy brought by RFID.

Even more troubling is the potential for outsiders to stalk these students when they leave school premises. School identification badges typically do not use security measures to protect information from skimming. A student’s identification number could be copied and stored, and anyone with an RFID reader could track students as they leave school grounds. This concern is amplified by the fact that use of RFID creates a false sense of security. A student who is separated from his or her RFID badge will register a false location. In its current form, RFID simply fails to make students safer and may create unintended security risks.

Increased Identity Theft

RFID chips can transmit personal information without our knowledge. “Passive” RFID chips transmit information whenever readers awaken them, while “active” RFID chips constantly transmit information. Neither technology is impervious to hacking or cloning. The cutting edge Dutch e-Passport’s RFID code was copied, stored and cracked in less than two hours by security experts, revealing the individual’s photograph and digital fingerprint. RFID is paving the way for a greater magnitude of identity theft than we have ever seen.
Profiling Consumers with RFID in Stores

Many businesses use RFID to track inventory and as a theft-deterrent. Certain RFID readers placed in a store are able to read all RFID tags present — not just in merchandise but in all RFID-equipped identification or credit cards. Currently, there is no requirement for retailers to disclose the location of RFID readers, or to remove or deactivate RFID tags after purchase.

As RFID tags become more prevalent, businesses can create profiles of consumer preferences and store massive amounts of data about who buys what products. Without guidelines about use of consumer data, there are no limits on aggressive and invasive marketing schemes.

CONCLUSION

RFID purports to bring greater security, but in practice results in greater risks. Enhanced driver’s licenses have the potential to speed border crossings, but they also heighten risk of identity theft. Individuals must be protected against unauthorized reading of their personal information.

Before issuing enhanced driver’s licenses or any other form of government identification with RFID, Texas should launch a study to further investigate the effects of RFID, and pay special attention to identity theft and safety risks.

RESOURCES


BACKGROUND

Americans have proudly rejected attempts to implement a national identification card throughout our history. Resistance to the Real ID Act is a natural extension of that history. Congress passed the Real ID Act in May 2005. It was tacked on to a bill that called for tsunami relief and military appropriations. There was limited debate on Real ID, and no one held hearings on the subject.

The Real ID Act creates an identity card that everyone living in the U.S. would be required to have in order to board a plane, enter a Federal building or go into a nuclear power plant. The intent of the Real ID Act is to prevent terrorism and reduce fraud, but Real ID will accomplish neither. It will result in high costs to states and individuals. Real ID will also do nothing to make Texans safer.

PROPOSALS

- **Pass** legislation refusing to comply with Real ID.
- **Decline** to fund the federal Real ID mandate.

EXPLANATION

Real ID legislation would affect 22 million Texans who currently hold driver’s licenses or identification cards issued by the Department of Public Safety. In March 2008, the U.S. Department of Homeland Security (DHS) released a revised cost estimate for Real ID legislation. The total cost is $9.9 billion, to be paid for by individuals ($5.8 billion), the states ($3.9 billion), and the federal government and private sector ($0.2 billion).

In Texas, Real ID will cost an estimated $129 million during its first two years of implementation. With only $80 million available through DHS grants, ordinary Texans would pay the difference. Compliance with the Real ID Act would result in the expansion of government to implement Real ID, as well as a massive national database that would render every American vulnerable to identity theft.
More Than a Hassle: Rising Costs & Expanding Bureaucracy

The Federal government estimates that Real ID will cost at least $9.9 billion, yet Congress has appropriated less than one percent of that amount. This fuels concerns that the federal government will pass along these burgeoning costs to states and individuals.

The Texas Department of Public Safety (DPS) acknowledges that implementation of Real ID will create challenges in Texas, with “operational, legislative, technological and fiscal limitations.” Implementation of Real ID will require additional personnel, facilities, training and technology. Texas will likely have to raise licensing fees to cover these additional costs, which will place a financial burden on ordinary Texans.

In addition to the financial burden of Real ID, Texans will be inconvenienced. They will have to apply for the Real ID in person. Alternate methods such as Texas Online, mail and telephone renewal will be discontinued during the Real ID implementation process. These methods save both time and money for Texans, and Real ID threatens to undo the progress Texas has made in recent years.

“Invasion of Personal Privacy and Risk of Identity Theft: At What Cost?”

If the initial cost estimate of Real ID was $23.1 billion, how did the revised estimate get reduced to $9.9 billion? Simply put, DHS decided to forego security measures on the Real ID because they were too costly.

Each Real ID will have a 2D barcode that will contain personal information, including the individual’s name, address, date of birth and a digital photograph. Against the recommendation of its own privacy experts, DHS opted to leave the barcode unencrypted, which means that anyone with a 2D barcode reader can capture and store the personal information of millions of Americans. These barcode readers are extremely common; the ubiquity of Real ID will result in widespread access to personal information by unauthorized third parties.

The Real ID Act also creates a massive, interlinked database that includes digital copies of personal documents like birth certificates. Alarmingly, there is no national security plan in place to protect personal information. Such a massive database is essentially “one-stop shopping” for identity thieves, and volumes of personal information would be highly vulnerable to insider and outsider fraud.

“While I support efforts to enhance our national security, it should not come at the loss of state sovereignty and the undue burden on our citizens.”

– Senator Craig Estes
High Stakes for Negligible Benefits

Security experts believe that any benefits that might result from Real ID—benefits that are negligible at best—will not be realized until December 2017 at the earliest.

It is not surprising that 11 states have passed laws that reject Real ID, and 21 states have passed either legislation or resolutions that reject it. These states understand that Real ID places an undue burden on their agencies and their citizens, and they have rightly chosen to oppose implementation of Real ID.

CONCLUSION

Texas is known for doing things its own way. Making Texans safer has always been a priority of policymakers, but Real ID legislation will achieve the opposite. Rejecting Real ID is the best way that lawmakers can ensure the safety and privacy of Texans, and avoid paying for a costly and burdensome unfunded federal mandate.

RESOURCES

American Civil Liberties Union, "Fuzzy Math and the Cost of REAL ID.
http://www.aclu.org/safefree/general/33690res20080116.html

Brendan McKenna, "States get a breather on starting REAL ID," Dallas Morning News (January 11, 2008).


http://www.estes.senate.state.tx.us/pr07/p031507a.htm

Texas Department of Public Safety: http://www.txdps.state.tx.us/oai/2009-2013/10externalassessment.pdf