Testimony of

Bruce Schneier

May 8, 2007

Testimony of Bruce Schneier
Security technologist, author, founder and CTO of BT Counterpane

"Will REAL ID Actually Make Us Safer?
An Examination of Privacy and Civil Liberties Concerns"

Senate Judiciary Committee
Room 226, Dirksen Senate Office Building

Tuesday, May 8, 2007

STATEMENT

I appreciate the opportunity to appear before the Committee today to discuss privacy issues. My name is Bruce Schneier. I am a security technologist, author, and CTO of BT Counterpane. The expertise I bring to this committee is less in the privacy and civil liberties realms, and more in the security realm. As such, I will focus my comments on the insecurities of the REAL ID system, the ineffectiveness of identity-based security systems, and the need to find smart and effective solutions to new security challenges. I'd like to emphasize at the start that this is an enormously interesting, important, and subtle topic, and I appreciate the decision of the Committee to hold these hearings.

The Electronic Privacy Information Center has coordinated comments to the Department of Homeland Security on REAL ID: signed by 21 experts on privacy and technology, including myself. I ask to submit it for the record.

When most people think of ID cards, they think of a small plastic card containing their name and a photograph. This isn't wrong, but it's only a small piece of any ID program. What starts out as a seemingly simple security device--a card that binds a photograph with a name--rapidly becomes a complex security system.

It doesn't really matter how well a REAL ID works when used by the hundreds of millions of honest people who would carry it. What matters is how the system might fail when used by someone intent on subverting that system: how it fails naturally, how it can be made to fail, and how failures might be exploited.

The first problem is the card itself. No matter how unforgeable we make it, it will be forged. The new U.S. $20 bill was forged even before it was released to the public. We can raise the price of forgery, but we can't make it impossible. REAL IDs will be forged. And, as I will show below, the fact that a REAL ID is a more valuable identification document than a driver's license means that it is more likely to be forged.

Even worse, REAL ID will not prevent people from getting legitimate cards in fraudulent names. Three of the 9/11 terrorists had valid Virginia driver's licenses in fake names, after bribing a DMV clerk. And even if we could guarantee that everyone who issued national ID cards couldn't be bribed, cards are issued based on other identity documents--all of which are easier to forge. REAL ID can be no more secure than the documents sufficient to get one.

And we can't assume that everyone will always have a REAL ID. Currently, about 20% of all identity documents are lost per year. An entirely separate security system would have to be developed for people who lost their card, a system that itself would be susceptible to abuse. Additionally, any ID system involves people: fallible people who regularly make mistakes. We've all heard stories of bartenders falling for obviously fake IDs, or sloppy ID checks at airports and government buildings. It's not simply a matter of training; checking IDs is a mind-numbingly boring task, one that is guaranteed to have failures. The anti-counterfeiting features of REAL ID are only as good as the verification mechanisms.

All of these problems demonstrate that identification checks based on REAL ID won't be nearly as secure as we might hope. But the main problem with any strong identification system is that it requires the existence of a massive database. DHS maintains that it's not one database, but fifty-plus separate databases. This is a semantic dodge; a series of interconnected physical databases is the same as a single massive database. In this case it's a massive database of private and sensitive information on every American--one widely and instantaneously accessible from airline check-in stations, police cars, schools, and so on.

The security risks of this database are enormous. It would be a kludge of existing databases that are incompatible, full of erroneous data, and unreliable. Computer scientists don't know how to keep a database of this magnitude secure. The daily stories we see about leaked personal information demonstrate that we do not know how to secure these large databases against outsiders, to say nothing of the tends of thousands of insiders authorized to access it. The fact that REAL ID database is a "one stop shop" for personal information exacerbates these risks.

Even worse, the residential-address requirement puts domestic violence survivors at risk, both by printing the information on the card and including it in the broadly accessible database.

REAL ID creates huge risks for privacy and security. Yet DHS has punted on privacy. The agency claims it doesn't have the power to require strong privacy protections, because the REAL ID Act did not explicitly say "DHS must set strong privacy protections for this massive trove of personal data." It is ludicrous for the DHS to suggest that it must be explicitly told to protect the personal information of Americans. DHS has an obligation to protect citizens, and cannot shirk that obligation.
But even if we could solve all these problems, we still wouldn't be getting very much security. A reliance on ID cards is based on a dangerous security myth, the idea that if only we knew who everyone was, we could pick the bad guys out of the crowd.

In an ideal world, what we would want is some kind of ID that denoted intention. We'd want all terrorists to carry a card that said "evildoer" and everyone else to carry a card that said "honest person who won't try to hijack or blow up anything." Then security would be easy. We could just look at people's IDs, and, if they were evildoers, we wouldn't let them on the airplane or into the

building.
This is, of course, ridiculous; so we rely on identity as a substitute. In theory, if we know who you are, and if we have enough information about you, we can somehow predict whether you're likely to be an evildoer. But that's almost as ridiculous. If you need any evidence of this, look at the single largest identity-based anti-terrorism security measure in this country: the No-Fly List. The No-Fly List has been a disaster in every way: it harasses innocents, it doesn't catch anyone guilty, and it is trivially easy to evade. This is what you get with identity-based security, and this is what you should expect more of with REAL ID.

Even worse, as soon as you divide people into two categories--more trusted and less trusted people--you create a third, and very dangerous, category: untrustworthy people whom we have no reason to mistrust. Oklahoma City bomber Timothy McVeigh; the Washington, DC, snipers; the London subway bombers; and many of the 9/11 terrorists had no previous links to terrorism. Evildoers can also steal the identity--and profile--of an honest person. And if you think it's bad for a criminal to impersonate you to your bank, just wait until a terrorist impersonates you to the TSA. Profiling can result in less security by giving certain people an easy way to skirt security.

Even if you could magically solve all of these problems, REAL ID would not have prevented 9/11. Three 9/11 terrorists used legitimate driver's licenses in fake names received by bribing a Virginia DMV clerk, something REAL ID would not prevent. Some used foreign passports, something that would not be prevented by REAL ID. And it makes no sense to focus on the particular tactics of the 9/11 terrorists when there were equally effective alternate tactics. Today, it is trivially easy to fly under someone else's name. Today--and forever in the future--anyone can fly without an ID.

Enough of terrorism; what about more mundane concerns like identity theft? Perversely, a hard-to-forge ID card can actually increase the risk of identity theft. A single ubiquitous ID card will be trusted more and used in more applications. Therefore, someone who does manage to forge one--or get one issued in someone else's name--can commit much more fraud with it. A centralized ID system is a far greater security risk than a decentralized one with various organizations issuing ID cards according to their own rules for their own purposes.

Security is always a trade-off; it must be balanced with the cost. We all do this intuitively. Few of us walk around wearing bulletproof vests. It's not because they're ineffective, it's because for most of us the trade-off isn't worth it. It's not worth the cost, the inconvenience, or the loss of fashion sense. If we were living in a war-torn country like Iraq, we might make a different trade-off.

Real ID is another lousy security trade-off. The last cost estimate I saw was $20 billion--and that makes unrealistic assumptions about IT projects being able to stay in budget--and we won't get much security in return. My recommendation is to scrap REAL ID altogether. For the price, we're not getting anywhere near the security we should.

Thank you for allowing me to address the committee. I welcome your questions.