Protecting privacy and liberty

The events of 11 September offer a rare chance to rethink public security.

Bruce Schneier

DAVID NEWTON

Appalled by the events of 11 September, many Americans have declared so loudly that they are willing to give up civil liberties in the name of security that this trade-off seems to be a *fait accompli*. Article after article in the popular media debates the 'balance' of privacy and security — are various types of increase in security worth the consequent losses to privacy and civil liberty? Rarely do I see discussion about whether this linkage is valid.

Security and privacy are not two sides of an equation. This association is simplistic and largely fallacious. The best ways to increase security are not at the expense of privacy and liberty. Giving airline pilots firearms, reinforcing cockpit doors, better authentication of airport maintenance workers, armed air marshals travelling on flights and teaching flight attendants karate are all examples of suggested security measures that have no effect on individual privacy or liberties.

Security measures that reduce liberty are most often found when system designers fail to take security into account from the beginning. They're Band-Aids, and evidence of bad security planning. When security is designed into a system, it can work without forcing people to give up their freedom. Take, as an example, securing a room. Option one: convert the room into an impregnable vault. Option two: put locks on the door, bars on the windows and alarms on everything. Option three: don't secure the room; instead, post a guard to record and check the identity of everyone entering.

Option one is the best, but is unrealistic. No vault is impregnable, getting close would be extremely expensive, and turning a room into a vault greatly reduces its usefulness as a room. Option two is the realistic best, combining the strengths of prevention, detection and response to achieve resilient security. Option three is the worst, as it is far more expensive than option two, and the most invasive and easiest to defeat of all three options. It's also a sign of bad planning: designers built the room, and only then realized that they needed security. Rather than installing door locks and alarms, they take the quick way out and invade people's privacy.

A more complex example is Internet security. Preventive countermeasures help significantly to protect sites against 'script kiddies' but fail against smart attackers. Detection and response are key to providing security on the Internet. My company catches hackers all the time, by monitoring the audit logs of network products: firewalls, IDSs, routers, servers and applications. We don't eavesdrop on legitimate users, read mail or otherwise invade privacy. We monitor data about data, and find abuse that way.

We detect yesterday's attacks by watching for their signatures, and tomorrow's by noticing and investigating anomalies. We can respond in time to thwart these attacks. This monitoring doesn't work automatically; it requires people to separate real attacks from false alarms, to investigate anomalies and to pursue attackers relentlessly. It's not perfect, but combined with preventive security products it is more effective, and more cost-effective, than anything else.

There are strong parallels between Internet security and the real world. All criminal investigations look at surveillance records. The lowest-tech version of this is questioning witnesses. In the current investigation, the FBI is looking at airport videotapes, airline passenger records, flight-school class records and financial records. The effectiveness of the investigation is directly related to the quality of the examination.

Some criminals and terrorists are copycats, who do what they've seen done before. To a large extent, this is what hastily implemented security measures try to prevent. But others invent new methods, as we saw on 11 September. We can build security to protect against yesterday's attacks, but we can't guarantee protection against tomorrow's: the hacker attack that hasn't been invented, or the terrorist attack still to be conceived.

Demands for even more surveillance miss the point. The problem is not obtaining data, it's deciding which are worth analysing and interpreting. Everyone leaves an audit trail through life; the FBI quickly pieced together the terrorists' identities once it knew where to look. More data can even be counterproductive. The National Security Agency and the CIA have been criticized for relying too much on signals intelligence, and not enough on human intelligence. The East German police collected data on four million people, yet they did not foresee the overthrow of the government because they invested heavily in data collection instead of interpretation. We need more intelligence agents on the ground in the Middle East debating the Koran, not sitting in Washington arguing about wiretapping laws.

People are willing to give up liberties for vague promises of security because they think they have no choice. What they're not being told is that they can have both. It would require us to discard the easy answers. It would require designers to build security into systems from the beginning instead of tacking it on at the end. It would require the structuring of incentives to improve overall security rather than simply decreasing its costs. And it would make us all more secure.

Some broad surveillance, in limited circumstances, might be warranted as a temporary measure. But surveillance should not be designed into our electronic infrastructure. As the saying popularized by Thomas Jefferson goes: "Eternal vigilance is the price of liberty." Historically, liberties have always been a casualty of war, but a temporary casualty. This war — a war without a clear enemy or end condition — has the potential turn into a permanent state of society. We need to design our security accordingly. ■

Bruce Schneier is at Counterpane Internet Security, 19050 Pruneridge Ave, Cupertino, California 95014, USA. This is an edited version of an article in Crypto-Gram *at www.counterpane.com.*