

Government-Run Cyber Security? No, Thanks

By *Jim Harper*

March 13, 2009

Most people assume, and it's probably true, that our nation's networks and databases aren't secure enough. The risks range from corporate espionage to data breach and identity fraud to "[cyber warfare](#)." The White House is [taking on this problem](#)-it's conducting a 60-day cyber security review. The review should explicitly deny federal responsibility for securing private infrastructure.

The president regards his budget as a "[blueprint for America's future](#)." His opponent in the recent election wanted to be [commander-in-chief of the United States](#). So it wouldn't be surprising if the review set the stage for a federal takeover of communications networks in the name of cyber security. But owning cyber security may be an unappealing prospect even for federal authorities with an expansive view of their roles. The surveillance needed for government-run cyber security would create prohibitive threats to civil liberties and privacy. And government folks seem aware that they don't know how to do cyber security any better than anyone else.

How do you improve security without exploding government power? How do you do it without giving the government de facto surveillance over the Internet? And, most importantly, how do you actually figure out how to do it?

The economic statement of the problem is this: Network operators, data owners, and users sometimes create externalities-risks to others that don't affect their own bottom lines. Getting them to internalize those risks can be done one of two ways: Regulation-you mandate it-or liability-you make them pay for harms they cause others. Regulation and liability each have strengths and weaknesses, but a liability regime is ultimately superior.

One of the main problems with regulation-especially in a dynamic field like technology-is that it requires a small number of people to figure out how things are going to work for an unknown and indefinite future. Those kinds of smarts simply don't exist. So regulators often punt: When the Financial Services Modernization Act tasked the Federal Trade Commission with figuring out how to secure financial information, it didn't. Instead, the "[Safeguards Rule](#)" simply requires financial institutions to have a security plan. If something goes wrong, the FTC will go back in and either find the plan lacking or find that it was violated, much like the [body-bagging the SEC does](#).

Another weakness of regulation is that it tends to be too broad. In an area where risks exist, regulators will ban entire swaths of behavior rather than selecting among the good and bad. In 1998, for example, Congress passed the Children's Online Privacy Protection Act, and the FTC set up an [impossible-to-navigate regime](#) for parental approval of the websites their children could use. Today, no child has been harmed by a site that complies with COPPA because there really aren't any. The market for serving children entertaining and educational content is a shadow of what it could be.

Regulators and regulatory agencies are also subject to "capture." In his recent [caution against network neutrality regulation](#), Tim Lee shows how industries have historically co-opted the agencies intended to control them and turned those agencies toward insulating incumbents from competition.

And regulation often displaces individual justice. The Fair Credit Reporting Act preempted state law causes of action against credit bureaus that, thus, cannot be held liable for defamation when their reports wrongfully cause someone to be denied credit. "Privacy" regulations under the Health Insurance Portability and Accountability Act gave enforcement powers to an [obscure office](#) in the Department of Health and Human Services. While a [compliance kabuki dance](#) goes on overhead, people who have suffered privacy violations are diverted to seeking redress by the grace of a federal agency.

Tort liability is based on the idea that someone who does harm, or allows harm to occur, should be responsible to the injured party. When a person drives a car, builds a building, runs a hotel, or installs a light switch, he or she owes it to anyone who might be injured to keep them safe. [A rule of this type could apply](#) to owners and operators of networks and databases.

A liability regime is better at discovering and solving problems than regulation. Owners faced with paying for harms they cause will use the latest knowledge and their intimacy with their businesses to protect the public. Like regulation, a liability regime won't catch a new threat the first time it appears, but as soon as a threat is known, all actors must improve their practices to meet it. Unlike regulations, which can take decades to update, liability updates automatically.

Liability also leaves more room for innovation. Anything that causes harm is forbidden, but anything that does not cause harm is allowed. Entrepreneurs who are free to experiment will discover consumer-beneficial products and services that improve health, welfare, life, and longevity.

Liability rules aren't always crystal clear, of course, but when cases of harm are alleged in tort law, the parties meet in a courtroom before a judge, and the judge neutrally adjudicates what harm was done and who is responsible. When an agency enforces its own regulation, it's not neutral: Agencies work to "send messages," to protect their powers and budgets, and to foster future careers for their staffs.

Especially in the high-tech world, it's hard to prove causation. The forensic skill to determine who was responsible for an information age harm is still too rare. But regulation is equally subject to evasion. And liability acts not through lawsuits won, but by creating a protective incentive structure.

One risk unique to liability is that advocates will push to do more with it than compensate actual harms. Some would treat the creation of risk as a "harm," arguing, for example, that companies should pay someone or do something about potential identity fraud just because a data breach created the risk of it. They often should, but blanket regulations like that actually promote too much information security, lowering consumer welfare as people are protected against things that don't actually harm them.

As complex and changing as cyber security is, the federal government has no capability to institute a protective program for the entire country. While it secures its own networks, the federal government should encourage the adoption of state common law duties that require network operators, data owners, and computer users to secure their own infrastructure and assets. (They in turn will divide up responsibility efficiently by contract.) This is the best route to discovering and patching security flaws in all the implements of our information economy and society.

The White House's 60-day cyber security review should explicitly deny federal responsibility for securing private communications infrastructure. This is the best way forward and an essential route if we are to keep the government from monitoring and controlling Americans' private communications.



[Jim Harper](#) is the director of information policy studies at the Cato Institute in Washington, D.C. To subscribe, or see a list of all previous TechKnowledge articles, visit [TechKnowledge Newsletter - Technology and Telecom Studies](#).

This work is licensed under a [Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International License](#).

PRINTED FROM CATO.ORG