Avoid Privacy Regulation that Could Worsen Personal Security

There are two great ironies in calls by lawmakers and consumer advocates to protect consumer privacy by regulating businesses that handle sensitive personal data. First, the most egregious privacy violations have historically been perpetrated not by businesses engaged in consumer transactions but by governments on their own citizens.

Second, those violations of privacy that *do* result from business and consumer transactions are vastly facilitated by the government's own efforts to collect individuals' personal information. Social Security numbers, names, and birth dates—the holy trinity of information for identity thieves—are all kept in government databases, and the federal government itself has promoted their use by financial institutions as identity verification.

Some lawmakers want to collect even more information into federally controlled databases encompassing all citizens. Others have proposed requiring either national ID cards or that state ID cards meet certain federal standards—which would make state IDs into de facto national IDs.

Yet that is not all. With homeland security becoming an increasingly important national policy issue, there will be a growing impetus to gather still more data on citizens, including proposals to incorporate new technologies like biometrics and radio frequency ID tags into proposals for ID cards. The key to securing data and privacy is not to give government ever more personal information, but less.

Government efforts to regulate private sector privacy standards are misguided. One-size-fits-all regulations are an ineffective means of maximizing privacy and security. The diverse uses for digital devices and networked communications create privacy and security needs that could not possibly be met by static laws enforced by distant bureaucrats. The appropriate level of privacy and data safety varies depending on the type of information—for example, a level of security that may be acceptable for an online sale on eBay may be inadequate for a computer system that operates a facet of critical infrastructure, such as a chemical or power plant. Similarly, the data transmitted between an individual and his local bank, although sensitive, may be far less sensitive than the data transmitted by a mutual fund manager or a doctor.

With technologies to secure privacy constantly improving, companies are developing techniques to ensure that sensitive data and networks are protected according to user preferences and needs. The market forces of competition and innovation are constantly helping businesses and consumers devise solutions to

new problems. Federal regulation could not anticipate and respond to the ever-changing threats to digital information, nor is regulation likely to encourage robust and competitive markets for privacy-enhancing products. Legislative mandates in computer security are more likely to stifle innovation and ossify technology standards.

Consumers today demand security in addition to functionality when it comes to online transactions and new gadgetry. As that demand grows, market institutions will evolve to produce even higher standards; insurance, company reputation, and third party watchdog groups are examples of market institutions that could negate the need for heavy-handed regulation. As technology advances, governments must constrain their own excesses by:

- Avoiding mandatory databases.
- Ensuring Fourth Amendment protections for public surveillance.
- Avoiding mixing public and private databases.

Beyond that, government involvement in private sector privacy and data security issues should be limited to:

- Enforcing the contractual obligations of both businesses and consumers with respect to information security procedures.
- Tracking and punishing the cyber-criminals responsible for data breaches and identity theft, rather than the companies victimized by such criminals.

Wayne Crews