Regulate Government Data Collection While Avoiding Prescriptive Privacy Regulation

There are two notable ironies in proposals by politicians and self-styled consumer advocates to protect consumer privacy by regulating businesses that handle sensitive personal data. First, the most egregious privacy violations are typically perpetrated not by firms, but by governments against their own citizens. Second, those violations of privacy that do result from business and consumer transactions are often facilitated by government.

The laws safeguarding individuals and businesses from unwarranted law enforcement access to sensitive information stored in the "cloud" (remote Internet-based servers operated by third parties) are woefully outdated. Today, government can compel service providers to disclose the contents of many kinds of private correspondence without first obtaining a search warrant or any other court order authorized by a judge. Lawmakers should revise U.S. electronic privacy statutes to better reflect the realities of the information age by applying robust protections to the contents of all private communications stored electronically.

Government routinely collects and stores individuals' personal information, including Social Security numbers, names, and birth dates—the holy trinity for identity thieves. In some cases, government has even promoted the use of these identifiers by financial and medical institutions. In the name of homeland security, some lawmakers hope to require citizens to disclose even more information that would be stored in federal databases. Some policy makers have proposed mandatory biometric national identification cards. Yet the real key to safeguarding our privacy is to grant government less access to ever more personal information, not more.

Federal efforts to regulate private sector privacy standards are fundamentally misguided. One-size-fits-all regulations that purport to increase privacy and security invariably have serious downsides. In many cases, privacy regulation actually renders sensitive information even more vulnerable. Evolving digital devices and telecommunications technologies are constantly creating new privacy and security concerns that cannot be properly addressed by static laws enforced by distant bureaucrats. The appropriate level of privacy and data security varies dramatically depending on the type of information in question and on the needs of every specific individual. No two consumers share the same set of privacy preferences. Flexible, voluntary private arrangements, bolstered by the competitive process, are the best means of effectively balancing privacy concerns against other vital interests as the information age evolves.

Technologies that enable users to safeguard their privacy on an individualized basis are

constantly improving. The perennial gale of competitive discipline continuously encourages businesses to devise better solutions to tough privacy problems. Federal regulation cannot anticipate or properly address the ever-changing threats to digital information. Legislative or regulatory mandates on data security are more likely to stifle innovation and ossify technology standard than to truly protect our privacy.

Consumers today demand both security and functionality in online commerce and communication. As the public grows more cognizant of privacy risks, market institutions evolve to create more robust and diverse privacy standards. These institutions—including insurance companies, reputational forces, and third-party watchdog groups—are all equipped to punish wrongdoers and incentivize smart privacy practices. And when private agreements are broken, government has an important role to play in allowing injured parties to obtain recourse through the judicial system.

Wayne Crews and Ryan Radia