The 21st Century Cures Act was hailed as the biggest health-care reform since ObamaCare. It's easy to see why: The law, which passed both houses of Congress by unanimous consent last December, increased the budget of the National Institutes of Health, designated nearly $2 billion for cancer research, and set aside $500 million in 2017 alone to address the opioid crisis.

Unfortunately, the legislation also weakened patients' privacy rights. Americans were already vulnerable under the Health Insurance Portability and Accountability Act of 1996. That law allowed government-funded researchers to collect and even share patients' medical and genetic information without their consent. But the 21st Century Cures Act goes further. In an effort to promote medical breakthroughs, the law tries to create an “information commons”: a government-regulated pool of data accessible to all health researchers, regardless of background, training or motive.

Although speeding research is a noble goal, there's little evidence that patients are willing to sacrifice their privacy the way that the 21st Century Cures Act requires. A 2007 survey by the Institute of Medicine found that only 1% of Americans were willing to have their health information shared for research without their consent. Yet the new law doesn't give patients in government-funded research any method to opt out of data sharing. It prohibits “information blocking” by health-care providers, essentially mandating that doctors and hospitals share data with government researchers. It encourages the creation of a “global pediatric clinical study network” to pool data on children world-wide.

Federal courts have upheld forced data sharing because patients “voluntarily”
give personal health information to their doctors. Some jurists and legal scholars, however, argue that today's laws don't adequately protect privacy. Consider the Supreme Court's unanimous 2012 decision in *U.S. v. Jones.* “It may be necessary,” Justice Sonia Sotomayor wrote in a concurring opinion, “to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties.” Although that case was about law-enforcement surveillance, Justice Sotomayor’s warning that the current privacy laws are “ill suited to the digital age” applies equally to medical research.

In theory, the data shared under the 21st Century Cures Act can’t be traced back to individual people. It’s stripped of direct identifiers like names, street addresses and Social Security numbers. But with big data virtually everything is traceable. A few years ago Harvard researchers examined about 600 anonymized profiles from a genome-research project. Participants had provided a few small pieces of information: birth date, sex and ZIP Code. By comparing that against public records and voter data, researchers were able to identify nearly half of these people by name. The same approach could work on medical records containing sensitive information about alcoholism, illegal drug use or sexual abuse.

Even if researchers stopped asking for birth date, sex and ZIP Code, anyone with an internet connection and a decent understanding of biology could link genetic data to individual patients. In 2013 a group of researchers led by MIT's Yaniv Erlich took anonymous genetic information and cross-referenced it against a public database genealogists use to match small differences in Y chromosomes with certain family trees. That helped establish the anonymous donors’ surnames, which were then cross-referenced with other public records, like voter and tax rolls. In this way the researchers were able to identify dozens of completely “anonymous” people.

The 21st Century Cures Act isn’t the only federal legislation that threatens patient privacy. A bill introduced in March by Rep. Virginia Foxx (R., N.C.), the Preserving Employee Wellness Programs Act, would give companies leverage to push genetic tests on their workers. Those who opt out could have their insurance premiums raised by up to 50%.

This genetic-testing requirement could quickly lead to discrimination, since companies would have an enormous incentive to avoid hiring people at high risk of serious illness. Although managers might never admit to firing people with risky genetic profiles, they could give these workers bad reviews or deny raises to force them to quit.

When the Founding Fathers wrote the Fourth Amendment, which protects against “unreasonable searches and seizures,” they were thinking of abusive government agents kicking down doors. But with modern technology, state officials and big companies don’t need to resort to brute force. In the internet age, they can get sensitive information from the comfort of their offices—and the law allows them to do just that.

*Ms. Brase, a registered nurse, is president of the Citizens’ Council for Health Freedom.*

*Appeared in the August 29, 2017, print edition.*