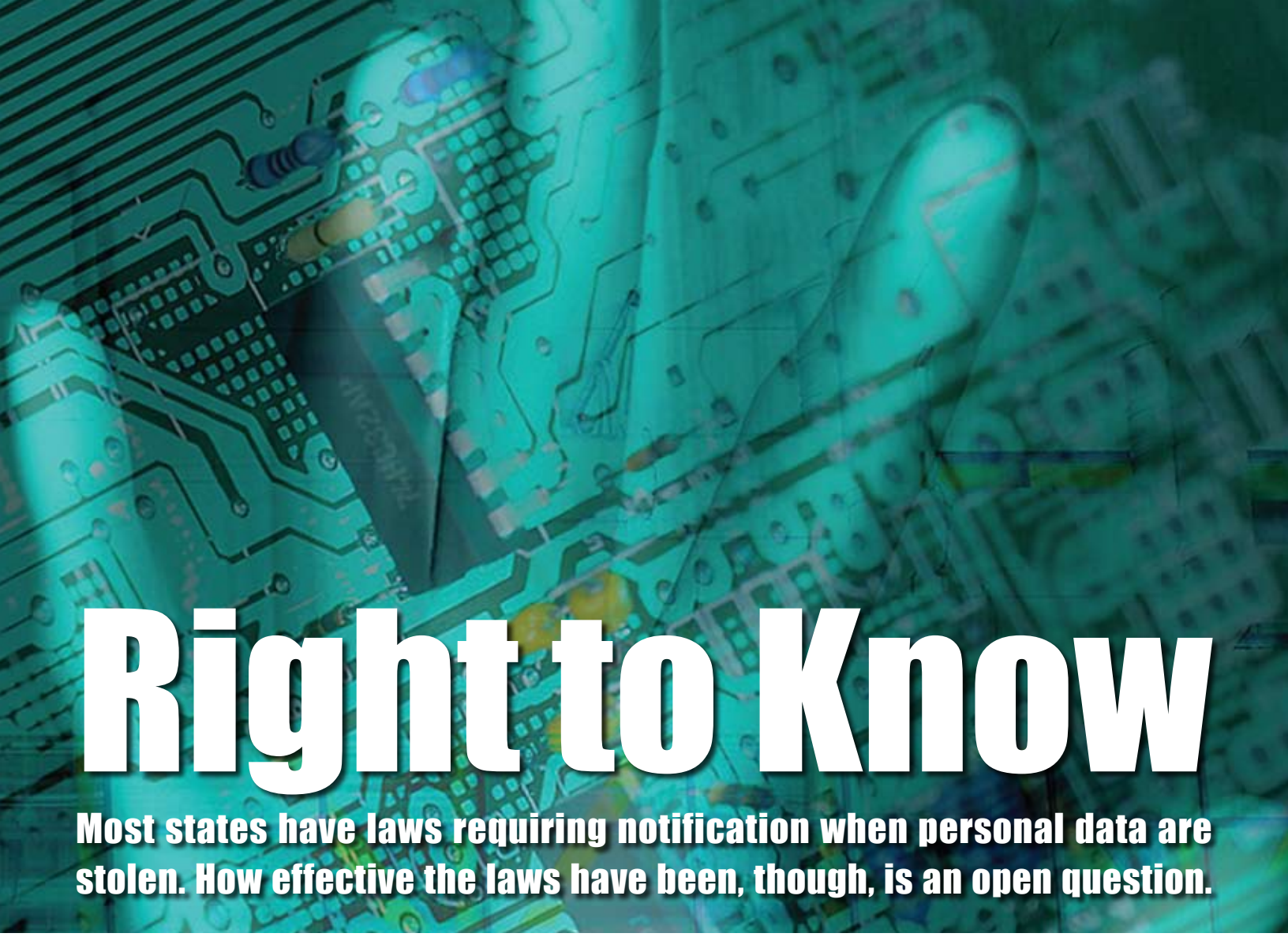


Right to Know

Most states have laws requiring notification when personal data are stolen. How effective the laws have been, though, is an open question.

BY PAM GREENBERG

A Countrywide mortgage employee working Sunday nights copied customer records from an office computer, then sold the personal information of an estimated 2 million mortgage applicants.

A group of hackers "wardriving"—searching for unsecured wireless networks in parking lots and outside retail stores such as TJ Maxx, Marshalls, Boston Market and others—managed to capture credit card numbers, passwords and account information for more than 40 million customers.

A laptop stolen from a National Institutes of Health researcher contained the information of about 2,500 participants in a medical research study, including names, birth dates, health data and diagnoses.

Before 2004, consumers rarely heard about these kinds of thefts. But a landmark California law, which went largely unnoticed outside the state when it passed in 2002, set off a chain of events felt nationwide. California's Security Breach Notice Law requires businesses or state agencies that have a security breach to notify state residents if their personal information is lost or stolen.

Since the law took effect in mid-2003, hundreds of data breaches have been reported in the press, and more than 245 million records containing personal information have been exposed. Thousands of people have received letters warning them to monitor their records, and businesses and organizations have beefed up data security. One study put the cost of data breaches to the companies involved at $197 per record breached in 2007.

NATIONAL REACH

In February 2005, ChoicePoint, a company that collects and compiles information about millions of consumers, discovered that it had inadvertently sold the personal information of almost 145,000 people to a con artist who claimed to be an executive with a Los Angeles company. ChoicePoint initially notified only California residents, who were covered by the state's notification law, even though the stolen data included information about residents in other states. Only after widespread media coverage, and after 38 state attorneys general had called for notification to victims in other states and territories, did the company notify everyone whose personal information had been compromised.

After ChoicePoint's security failure became widely known, lawmakers in other states moved quickly to make sure their citizens had the same kind of notice as California residents.

Twenty-two states enacted security breach laws in 2005, and others quickly followed in subsequent years.

Pam Greenberg covers Internet and computer security issues for NCSL.

In the five years since the California law has been in force, 43 states, the District of Columbia, Puerto Rico and the Virgin Islands have passed similar laws. But the laws have their critics, and researchers are beginning to take a careful look at their effectiveness.

LAWS CREATE CHANGE

"The law has worked surprisingly well," says Senator Joe Simitian, a sponsor of the California bill. "Millions of American consumers have known when their personal information had been disclosed and they were at risk."

With notice, a consumer can protect against theft by closing accounts, freezing credit reports—effectively blocking the issuance of new credit without permission—or issuing a fraud alert requiring creditors to check before extending any new credit.

The law also creates a powerful incentive on the part of government and business to improve data security. "You have a responsibility to handle this data with care, and if you come up short," Simitian says, "you'll suffer the damage to your reputation."

Companies have increased security practices in response to data breach laws, according to Chris Hoofnagle, director of Information Privacy Programs at the Berkeley Center for Law & Technology, who supervised a survey of chief security officers by the Samuelson Clinic. "Businesses are changing practices and policies, getting security on the accounting books, and integrating security into legal and marketing teams," he says.

Joanne McNabb, chief of California's Office of Privacy Protection, also sees businesses changing their practices. "One of the striking lessons we've learned is how much sensitive information is not safe on a server but is traveling on a laptop or flashdrive. It's now becoming a common practice to encrypt these and to have policies that restrict or limit what kind of information can be carried on these devices."

McNabb points to another change that's happening in government and the private sector. "There's a real scouring of systems to remove Social Security numbers. Organizations are saying, why do we still collect this or why are we keeping this information so long?"

A 2008 review of breach incidents compiled by the Privacy Rights Clearinghouse found that about 75 percent of the publicly known breaches involved Social Security numbers. A report by McNabb's office highlights how, after one university's breach had exposed Social Security numbers and other information from 15 years prior, it changed its policies to shorten the time it retained information on certain applicants. In another example, a blood bank stopped collecting Social Security numbers altogether.

SENATOR
JOE SIMITIAN
CALIFORNIA

CALIFORNIA SETS STANDARD FOR PRIVACY BREACH LAWS

When it comes to drafting security breach statutes, most states have taken California's law as the model.

There are, however, notable variations. All the security breach laws define "personal information" as a person's name in combination with a Social Security number, driver's license or ID card number, or financial account numbers. But 15 states have expanded the definition to include information such as account passwords or access codes, digital signatures, or passport or taxpayer ID numbers.

Arkansas, California and Puerto Rico have a broader definition of personal information that includes personal medical or health insurance information. Iowa, Nebraska, North Carolina, Texas and Wisconsin laws protect biometric data, such as a fingerprint or retinal image, if released with other personal information.

Every state except Wyoming exempts companies from reporting a breach if the personal data released are encrypted. The state laws usually apply only to computerized data, but Alaska, Hawaii and South Carolina also cover paper breaches.

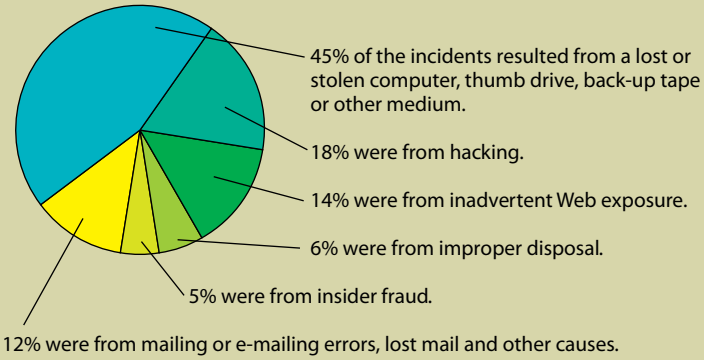
All the state laws require companies (and, in about half the states, government entities) to notify individuals directly in writing, by telephone or, in some circumstances, by e-mail, if their personal information has been compromised. Utah allows companies to disclose a breach through publication in a newspaper of general circulation in lieu of personal notice.

Eight states—Hawaii, Maryland, Michigan, New Hampshire, North Carolina, Oregon, Vermont and Wyoming—require businesses to include in the notice specific information about the breach, such as the type of information that was compromised, advice about precautionary actions to take, or a telephone number the consumer may call for further information and assistance.

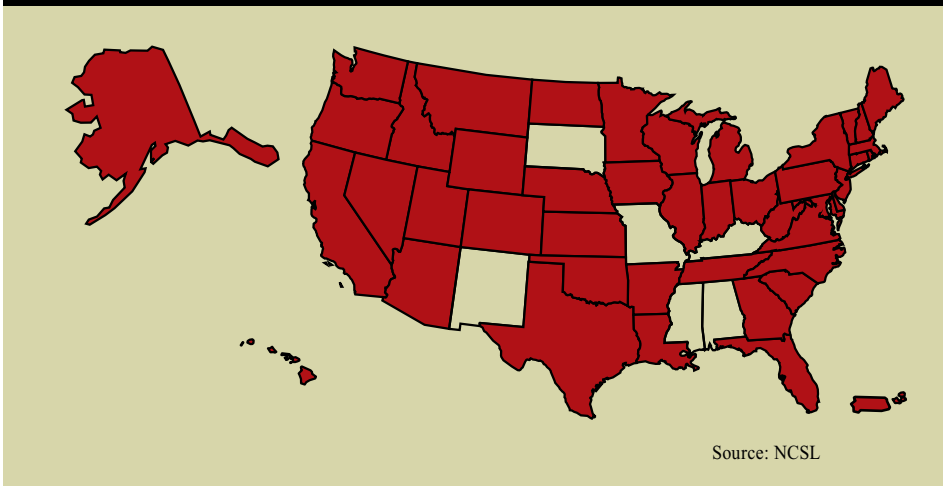
Hawaii, Maine, Massachusetts, New Hampshire, New Jersey, New York, North Carolina, Virginia and Puerto Rico also require businesses to report the breach to the attorney general or to a central state office in addition to providing notice to individuals.

HOW DATA ARE BREACHED

A 2008 review of 880 breach notifications by the Privacy Rights Clearinghouse made these findings:



STATES WITH SECURITY BREACH LAWS



Source: NCSL

CRITICS POINT TO LIMITATIONS

Some researchers, however, are questioning the benefits of the laws. A Progress and Freedom Foundation analysis of security breach laws questions whether the costs of notification outweigh the benefits. The report's authors, Thomas M. Lenard and Paul H. Rubin, maintain that businesses already have strong incentives to spend money on data security, because many of the costs related to identity theft and fraud are borne directly by business. They also argue that the benefits of the notice to consumers are negligible since only a very small percentage of those who receive breach notices actually become victims of a fraud.

Fred Cate, a law professor and director of the Center for Applied Cybersecurity Research at Indiana University, agrees. "Research shows pretty clearly that there's very little identity theft that follows breached accounts. Security threats are all around us, but security breaches are like a little sideshow. I don't mean to suggest that they aren't a concern, but if you asked security experts to name the top 15 security risks, I doubt breaches would be on anyone's list."

Also, a little less than half of consumers fail to take action after being notified that their information has been lost or stolen. A 2005 survey of identity theft victims by the Federal Trade Commission found that 44 percent did nothing after receiving a notice about a breach of their information.

"Notices have become a substitute for real action," Cate says.

But Simitian considers notices valuable, giving consumers the opportunity to take steps if they choose. "What you don't know can hurt you. You and I may get the same notice letter, and you may close all your accounts and do everything possible to protect yourself. Someone else may do nothing. I'll take a middle position and monitor my accounts more carefully."

Simitian also thinks notices can be improved by providing standard information about what data were breached.

McNabb agrees. "If the breach involves use of credit card numbers, you know the fraud is likely to happen fairly soon, and you can close your account. But with a Social Security number, there are numerous types of fraud that can occur, it can happen anytime, and you can't change your Social Security number."

EFFECT ON IDENTITY THEFT UNCLEAR

According to the most recent figures from the Federal Trade Commission, 8.3 million Americans were victims of identity theft in 2005, and identity theft is the No. 1 source of consumer fraud complaints the agency receives. And given the hardship that identity theft can create for individuals, it's not surprising that some have looked to security breach laws as a solution.

But data breaches are not the only ways in which identity theft occurs. A lost or stolen wallet or thefts from mail or garbage also can lead to identity theft. In addition, information about such thefts are often based on anecdotal

accounts or surveys of victims, who sometimes have no idea how their information was compromised.

"It's a fundamental problem that security breach laws have been hung on the hook of identity theft," says Hoofnagle. "Investigating the source of identity theft is extremely tricky."

A team of researchers at the Heinz School of Public Policy and Management at Carnegie Mellon has attempted to do so, however. The researchers compared identity theft rates, over time, in states with and without security breach laws, and concluded that data breach disclosure laws have "no statistically significant effect" in reducing identity theft.

The study also noted that, if a small percentage of identity thefts is attributable to data breaches, the effectiveness of data breach laws on these thefts is limited. The researchers acknowledged, however, a need for better data and further study. They also say security breach laws may have other benefits, such as reducing a victim's average losses and improving security practices.

LESSONS LEARNED

What have we learned after five years?

"We've learned that the law works well, but that there are some improvements that would make a good law even better," says Simitian.

In addition to requiring a core set of information in notice letters, Simitian favors requiring businesses to notify a central state entity. New York, for example, requires notification of breaches to the attorney general's office.

"It gives law enforcement the information they need to assess the particular kinds of data lost or the means by which they are being breached."

State lawmakers also need this information, he says. "If we're to legislate effectively, we need to know the nature and extent of the problem."

Cate is skeptical that including a standard set of information in letters will make a difference, but he supports the idea of a central reporting requirement. A central repository would have all the benefits of notice, he says, "without scaring people about dangers when no real harm is there or if there's little they can do about it."

With central reporting, businesses could start making more rational investments in security, says Hoofnagle. "I think we'll find these laws sparked investment and innovation in security—maybe even over-investment—but we were in a posture of under-investment before."

As states continue to work on improving data breach laws, Congress also has been considering legislation. Some bills have made it out of committee, but none have had a floor vote.

Federal legislation is a mixed blessing," says Simitian. "If we end up with a weaker set of provisions that also preempts the more rigorous state laws, that's not going to benefit consumers."

Cate thinks Congress will act, and he's surprised it hasn't already. "It's probably because they found it a lot more complicated than they thought."

The way data are collected, used and transferred across states, it's likely many companies will opt to comply with the most stringent provisions in state laws, Cate says.

"One way or another, we'll have national preemption—either from the state that adopts the toughest law or from Congress. But it's a classic case of states leading the way."

CHECK OUT steps Nevada and Massachusetts have taken to use encryption to keep private data safe. Also, we offer more details about privacy breach laws, identity theft and financial privacy laws at www.ncsl.org/magazine.