

8ghel339rtj23szxyt7ruji9jeuw76jhz7kl0oi2sdfxyychsocialSecurity  
8798df34zyYhkk647sg8jwyter5F7hjSty55yz78oPzyukjhqwyu45Hjhka  
26-05-7543JoeSmith//Securezs75chfih34t58oix8s3cyh87SS#636-03-  
e87yujkqw3hj69Dre89k//DOB02/12/1956//yoozwerte4tyox34n87xz  
Dworanitou//Securexhozhn348buzo6sdw3822kjw0wacliqw7845279  
oowerte4tyox34n87xzmnu4vwyard541zs75chfih34t58oix8s3cyh8//  
78ghel339rtj23szxyt7ruji9jeu//DOB:04/29/1955//w76jhz7kl0oi2sd  
eSecure45zyretrouterDNS1200zY0023//SS#896-32-6587JaredSolli  
erte4tyox34n87xzmnu8ghel339rtj23szxyt7ruji9  
hz7kl0oi2sdfxyychsocialSecurit//SS#325-65-8899JohnSmith8ghel3  
hz7kl0oi2sdfxyychsocialSecurityYsetr87k//DOB:08/16/1971//  
oteServerDNS2398798df34zyYhkk647sg8jwyter5F7hjSty55yz78oP  
5HjhkandSwi47zer007//SS# JoeSmith//Securezs75ch  
#636-03-9712MarryDoe//SS#425-07-0478//DOB:11/07/1973  
yujkqw3hj69Dre89kyoozwerte4tyox34n87xzmnu45szedSS#989  
Securexhozhn348buzo6sdw3822kjw0wacliqw784527973cvewz3r  
87xzmnu4vwyard541zs75chfih34t58oix8s3cyh8//SS#  
78ghel339rtj23szxyt7ruji9jeuw76jhz7kl0oi2sdfxyychsocial  
kcha-ingeserverSecureClement45zyretrouterDNS1200zY0023//SS  
39kyoLzwerte4tyox34n87xzmnu8ghel339rtj23szxyt7ruji9jeuw7  
uritylri4o//SS#325-65-8899JohnSmith8ghel339rtj23szxyt7ruji9j  
xyuRemoteServerDNS2398798df34zyYhkk647sg8jwyter5F7hjSty  
i47zer00e//SS# JoeSmith//Securezs75chfih34t58oi  
//Secure87aujkqw3hj69Dre89kyoozwerte4tyox34n87xzmnu4  
woranitou//Srcurexhozhn348buzo6sdw3822kjw0wacliqw  
3cvewz3re89iyoozwerte4tyox34n87xzmnu4vwyard541zs75chf  
15-4532JoeBlaw34yze5078ghel339rtj23szxyt7ruji9jeuw76jhz  
serverSecure4nzyretrouterDNS1200zY0023//SS#896-32-6587  
te4tyox34n87xzanu8ghel339rtj23szxyt7ru//DOB:01/23/1942/  
jhz7kl0oi2sdfxyychsocialSecurit//SS# JohnSmit  
rtj23szxyt7ruji9jeuw76jhz7kl0oi2sdfxyych  
rityYsetr87kjxyuRemoteServerDNS2398798df34zyYhkk647sg8  
hjSty55yz78oPzyukjhqwyu45HjhkandSwi47zer007//SS#626-  
eSmith//Securezs75chfih34t58oix8s3cyh87SS#636-03-9712M  
Dre89kyoozwerte4tyox34n87xzmnu45szedSS#989-53-769  
0wacliqw784527973cvewz3re89kyoozwerte4tyox34n87xzm  
58oix8s3cyh8//SS#555-15-4532JoeBlaw34yze5078ghel339rt  
i2sdfxyychsocialSecurit1ExchangeserverSecure45zyretroute  
ujkqw3hj69Dre89kyoozwerte4tyox34n87xzmnu8ghel339rt  
uji9jeuw76jhz7kl0oi2sdfxyychsocialSecurit//SS#325-65-88  
ruji9jeuw//DOB:04/05/1923//76jhz7kl0oi2sdfxyychsocialS  
ruji9jeuw//DOB:04/05/1923//76jhz7kl0oi2sdfxyychsocialS

# INTO THE BREACH

How a last-minute comment by a Boalt professor to a Boalt alumnus helped produce one of the most powerful pieces of cybersecurity legislation to date.

*By Bonnie Azab Powell*

**B**ack in February 2002, a year after being elected to the California Assembly, Joe Simitian '77 arranged a conference call with two trusted legal experts in online privacy. The 11th District's state senator since 2004, Simitian has a master's in urban planning from UC Berkeley in addition to his J.D. from Boalt, and another in international policy studies from Stanford. (When asked whether he wears red or blue to the Big Game, he takes a polite Fifth.) The freshman assemblyman from Silicon Valley had been following the issue as an "interested member of the public," he says, and as a result had volunteered to chair a new Select Committee on Privacy. He was looking for a relatively narrow way to advance consumer protection that would have high prospects of passing as legislation—"a slam dunk," in his words.

Forty-eight hours before the legislative deadline, Simitian had decided on a bill: Entities collecting personal identifying information online from Californians would have to post a privacy policy—

and comply with it. All that remained was to run it past his informal advisers: Boalt Professor Deirdre K. Mulligan, director of the Samuelson Law, Technology & Public Policy Clinic, and Chris Kelly, then at a technology law firm and currently the chief privacy officer of social networking giant Facebook.

Mulligan and Kelly both said the bill was a “good first effort”—and one that had reasonable prospects of passage, recalls Simitian. He asked what else was on their wish lists to improve consumer protection online.

Mulligan immediately suggested that Simitian add a “security breach notification” provision to the proposed bill, which would require companies to notify people in the event of unauthorized access to their confidential personal information. While Mulligan was serving on a 1999 Federal Trade Commission advisory committee on online access and security, she was dismayed to learn about what she termed “real under-investment” in data security in the corporate sector. She knew the situation hadn’t improved—there was no business incentive to spend money on such safeguards without tangible benefits.

Simitian had already considered the breach angle but his discussions with industry led him to believe that it wouldn’t fly. But he figured that by taking Mulligan’s advice, he would have a disposable bargaining chip to help negotiate the privacy-policy requirement’s passage. He then suggested some possible breach notification guidelines and penalties.

A “light touch” would work better, countered Mulligan. “I said it should be a really minimal, low-intervention thing—simply that regardless of the reason for the breach, they would have to let their customers or patients know about it.”

“OK,” the assemblyman told Mulligan and Kelly. “Let’s go for it.” The next day, he introduced Assembly Bill 2297, “The Online Privacy and Disclosure Act of 2002.”

## Ignorance is not bliss

As it turns out, the bill was slightly ahead of its time. Back in early 2002, many state legislators weren’t even using email, let alone fretting about the security of personal information stored online. AB 2297 barely garnered enough votes to move on to the next stage—consideration by a California state senate committee. Then, on May 7, officials at the Stephen P. Teale Data Center in Rancho Cordova—one of two major providers of IT services to the State of California—realized that the state’s personnel database had been penetrated. A full month earlier, on April 5, hackers had gained access to the financial information of all 265,000 state workers. As it turned out, the breached files contained personal data for more than 100 California legislators: 80 assembly members and 40 state senators.

“We hit the jackpot, in terms of member interest and attention,” Simitian chuckles.

Senator Steve Peace, a veteran 20-year legislator who happened to be chair of the Senate Committee on Privacy, was among those wondering why it took Teale officials two weeks to notify state employees of the breach. During the lag, there had been several unauthorized attempts to access employees’ accounts, such as changing the address on a credit card. Peace immediately wanted to propose legislation requiring swift notification, but discovered that Simitian was ahead of him in the Assembly with his own version. Nearing the end of his final

term, Peace agreed to a compromise: He and the assemblyman would both “gut and amend” existing bills (that is, strip them of their content and insert new language, thus avoiding the delay required to introduce new bills) so that a pair of identical breach-notification versions, crediting Peace and Simitian as co-authors, would make their ways simultaneously—and quickly—through the California Senate and Assembly.

Still hoping to pass AB 2297, Simitian decided to gut and amend AB 700, a dormant bill regarding digital signatures he had introduced previously. His fellow legislators—now outraged data-theft victims—greeted both Simitian’s retrofitted AB 700 and Peace’s counterpart, Senate Bill 1386, with understandable enthusiasm. “Even Republicans saw this was a train they better get on,” recalls Simitian; they were pleased that the law would apply not only to the private sector, but also to state agencies, hospitals, and universities.

After swift approval, the bills were signed by then Governor Gray Davis as the Security Breach Information Act, which took effect July 1, 2003. California state law now requires “any person or business that conducts business in California” and that “owns or licenses computerized data that includes personal information” to notify all affected California residents in a “timely manner” if that personal information “was, or is reasonably believed to have been, acquired by an unauthorized person.” The state considers sensitive data to be a name plus a Social Security, driver’s license, credit-card, or other financial-account number.

Fundamentally, says Simitian, “Ignorance is not bliss. What you don’t know can hurt you. Consumers can’t protect themselves if they aren’t aware of the fact that they have been put at risk.”

## Tales from the encryption

The first achievement of California’s Security Breach Information Act was to motivate companies to take a good hard look at their practices. That came as no surprise to Mulligan. Her seemingly off-the-cuff suggestion to Simitian for light-touch legislation was actually an inspired strategy to get the data collectors to step up. “Rather than government setting guidelines and penalties, industry is in the best position to figure out how they can reduce security incidents,” says Mulligan.

She bases her reasoning on the effectiveness of the Environmental Protection Agency’s Toxic Release Inventory database, which requires companies to report accidental spills or leaks of hazardous materials above a certain threshold into the water, soil, or air. “That law was the most effective thing that had ever happened in the context of environmental policy with respect to getting firms to reduce emissions,” she says. “It’s credited for leading a race to the top. Instead of saying, do X, Y, or Z, it just says, ‘When you don’t perform well, let us know.’ Nobody wants to say, ‘We messed up.’ This motivates companies to constantly reassess their risk and the technology they’re using.”

In October 2003, just months after the new law took effect, the California Office of Privacy Protection, working with industry, state, legal, and consumer representatives, released a set of “recommended practices” governing data collection and breach prevention, preparing for a notification in case of a breach, and the actual notification. Among the guidelines, which were updated in April 2006 and February 2007, is the recommendation that

businesses collect only enough sensitive data “to accomplish your business purposes, and retain it for the minimum time necessary”—and to use data encryption wherever feasible. (The new law exempts businesses from having to notify consumers if the data obtained during a security breach, such as a stolen laptop, is unusable by the perpetrator.)

In December 2007, the Samuelson Law, Technology & Public Policy Clinic released a study of the effects of California’s and similar laws authored by Olive Huang ’07 and supervised by Chris Jay Hoofnagle, senior staff attorney at the Samuelson Clinic. The study is part of a comprehensive research initiative regarding chief security officers (CSOs) that is now under way at the Samuelson Clinic led by Mulligan and BCLT fellow Aaron Burstein ’04. It was a companion piece to a study of chief privacy officers (CPOs) headed by Mulligan and Boalt professor Kenneth A. Bamberger.

All of the seven CSOs interviewed by Huang (one at a nonprofit and six at publicly held companies) told the researchers that despite the minimal bite of the California law, it worked. It has, for example, prompted many more organizations to adopt data encryption, a technology that had previously been seen as too expensive. It has also reoriented many organizations’ approach to privacy away from solely focusing on compliance toward risk management of a valuable asset.

Security breaches, and notifying consumers about them, end up costing companies a lot of money. A 2005 Ponemon Institute study found that direct costs from breaches at 14 companies surveyed totaled nearly \$70 million, or \$50 per lost record. Indirect costs—such as time, effort, and other organizational resources expended—bring that rate to \$64 per lost record. Costs can include those incurred by setting up call centers, hiring legal counsel and defense services, and compensating victims—as well as lost business opportunities.

That certainly makes encryption look more attractive financially. A research group cited in the Samuelson study estimates that an encryption appliance for protecting large data-processing systems (100,000 or more customer records) would cost \$500,000 for initial setup, or about \$5 per account for the first year, then drop to \$1 per account per year in recurring costs.

The cost of a breach, while significant, is not the primary

motivation for an organization to get tough about its security, the Samuelson report finds. The biggest incentive is fear of the potential damage to its good name. “No one wants to have their organization on the front page of the newspaper,” the report quotes the interviewees as saying unanimously and almost verbatim.

“It’s a huge reputational hit,” agrees Barbara Lawler, CPO at the financial software and services company, Intuit. Lawler, then CPO at Hewlett-Packard, helped draft the California Office of Privacy Protection’s recommended breach notification practices. “Until these laws came into play, it was certainly more comfortable to think, ‘Well, that’s not going to happen to us.’ Technology and processes work, but occasionally they don’t; as long as you have humans involved, you have to be prepared.”

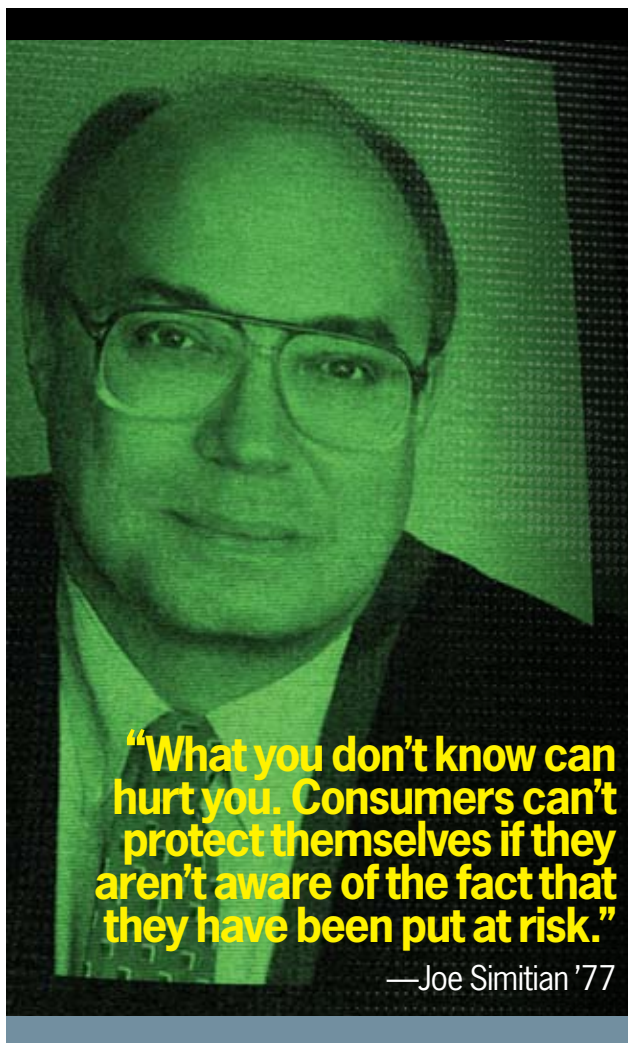
And in fact, it has been human error—not hackers—that has caused some of the biggest breaches in recent years. In February 2005, for example, the data collector ChoicePoint accidentally sold the personal information of 145,000 people to a criminal enterprise. And in May 2006, a laptop containing 26.5 million veterans’ data was stolen from a Veterans Administration employee’s home.

### The national trust

California’s simple notification law has had an enormous

impact across the country. Thirty-nine states, plus the District of Columbia, have since followed the trail that California blazed and enacted some form of breach-notification laws, with more in the pipeline. “About 25 percent look just like California, but the other 75 percent have a different twist,” says Lawler. The laws in Illinois and Delaware, for example, apply to anyone who handles, collects, or otherwise deals with personal information, while Georgia’s applies only to a much smaller subset covered under its definition of “information brokers.” The baseline for what is considered a breach vary from state to state, and some require notification only if there is what they deem a high or reasonable probability of identity theft.

Widespread adoption of the Internet as a business platform means that most companies and organizations now operate nationally and as a result find themselves sorting through and attempting to comply with a hodgepodge of state laws. Some simply set and try to meet the highest possible standard and send



out notifications even when doing so might not be necessary—which can be a problem in itself. Too many notices can lead to “envelope fatigue” on the part of consumers, and cause them to fail to act to protect themselves even when a serious breach occurs. Doing the minimum can backfire as well. In the heavily publicized ChoicePoint incident, the company first disclosed the breach only to California residents, even though it later revealed that residents in other states were also affected by the sale of their data to the criminal organization.

“A national standard would provide consistency for business and also pull in those edge riders so that everyone is obeying the same standard,” says Lawler, Intuit’s CPO. “It would mean that companies could act faster after a breach, which is absolutely a benefit for consumers.”

The Samuelson Clinic’s researchers agree—some-what. The CSO report concludes that while California’s Security Breach Information Act was an excellent first step for companies to get serious about protecting their data, more legislation is critically needed to standardize requirements to disclose a breach, ensure that consumers are notified in a clear, actionable manner, to centralize data collection on the nature and severity of the breach, and to make the data available to the public—so that industry and government can learn from each others’ failures and the public can assess which companies are doing a better job protecting their sensitive data.

On the federal level, six Senate (including one by California senator Diane Feinstein) and six House bills were introduced last year dealing with information security breaches. Three of them, all purporting to help prevent and mitigate identity theft, have made it out of committee and are on the Senate’s legislative calendar for debate.

## Hacks to the future

Simitian and Peace have received national recognition for their pioneering role in cybersecurity. Both were named among *Scientific American’s* 50 most outstanding leaders in science and technology in 2003; Simitian also received the 2007 Excellence in Public Policy Award at the 2007 RSA cybersecurity conference.

Simitian has introduced Senate Bill 364, which would once again put California on the cutting edge by addressing the

Samuelson CSO report’s last two points. SB 364 seeks to amend the existing breach-notification laws to require companies to report such breaches in plain English. (The Samuelson Clinic is collecting and studying notification letters, finding that many are written in legalese that may confuse consumers and even obscure the seriousness of a breach.)

“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,” Simitian told his fellow legislators in late January. “They are very simple: Provide greater clarity about what ought to be in that notice, and make sure that news of that security breach

also is reported to the state. The benefits: greater ability by consumers to protect themselves, greater clarity for businesses [...] and the ability of law enforcement, looking at a central repository, to understand if there are patterns or practices that they should identify and pursue.”

If passed, Simitian’s new bill would mandate that breach-notification letters include, at a minimum, some basic commonsense information: the toll-free telephone numbers and addresses of the major credit reporting agencies, the name and contact information of the reporting agency, a list of the types of information compromised; the dates of the breach, its discovery, and its notification; and the estimated number of people affected. SB 364 also requires companies to notify not only consumers, but also California’s Office of Information Security and Privacy Protection.

A section establishing a Web site to make all such notifications publicly available was excised due to budgetary pressure.

At press time, the amended bill had passed the California State Senate and was awaiting consideration by the Assembly. If the Assembly votes aye, and the governor signs it, Simitian and the Samuelson Clinic will have another feather in their caps in their quest to protect consumers.

“Technology changes. The law has to keep pace,” says Simitian. “And we learn by experience. What we learn then gets folded into the next generation of legislation.”

*Oakland freelancer Bonnie Azab Powell has written about the technology business for Red Herring, The New York Times, and Corporate Board Member, and about food for various national publications.*



**“Rather than government setting guidelines and penalties, industry is in the best position to figure out how they can reduce security incidents.”**

—Professor Deirdre K. Mulligan

# NAMING AND SHAMING

A Boalt research fellow exposes major institutions' failure to protect customers.



**“Until banks are forced to report the truth, identity theft will continue to fester in the dark.”**

—Chris Jay Hoofnagle

Representatives from major banks and telecommunications corporations woke up on February 27 to a public-relations nightmare. That’s when a brand-new report titled “Measuring Identity Theft at Top Banks (Version 1.0)” began making headlines, thanks in particular to several eye-catching charts. A number of the biggest names were reported as having failed spectacularly at protecting consumers from financial fraud, including Citibank, which has run a popular, humorous ad campaign touting its identity-theft protections. Among top banks, ING Direct, a “virtual bank” subsidiary of a Dutch conglomerate, emerged as having the lowest number of identity theft events.

The findings are just the first name-and-shame salvo in one man’s battle to measure the size and scope of identity fraud in this country. Given the proper tools, consumers can “vote with their feet and choose safer

institutions,” says Chris Hoofnagle, a consumer-privacy expert and senior fellow at the Berkeley Center for Law & Technology (BCLT).

No one knows how many billions of dollars are lost each year, because businesses aren’t legally required to disclose such losses. “Until banks are forced to report the truth, identity theft will continue to fester in the dark,” Hoofnagle argued in a 2007 *San Francisco Chronicle* editorial.

The Federal Trade Commission’s (FTC) policy had been to release only general trend data; the agency had never before identified institutions. Frustrated, Hoofnagle filed a Freedom of Information Act request with the FTC, settling for three randomly chosen months of 2006, with data on 88,560 complaints submitted by identity fraud victims.

The FTC’s data also doesn’t capture synthetic-identity theft, which may account for as much as 88 percent of all identity-related fraud, according to Hoofnagle. Syn-

thetic fraud differs from more familiar forms of such scams because consumers may never realize that they are victims. The con artists construct a fictitious identity by combining personal data from one or more consumers—typically a real Social Security number—with invented names, addresses, or other data. In their rush to grant instant credit, many institutions do not adequately check up on such red-flag mismatches.

Which is why Hoofnagle’s next target is the credit card companies. He predicts that credit unions will come out looking the safest in the new study. “The bigger banks are engaged in broader, and thus much riskier, marketing strategies,” he explains, pointing out that the institutions aren’t just exposing themselves to risk: taxpayers end up subsidizing fraud losses through lenders’ write-offs against their taxable income. “They need an incentive to heed the red flags.” —B.P.

## Events per month among institutions with high number of complaints\*

\*Average Events for Jan., Mar., Sept. 2006

