UCB SECURITY BREACH NOTIFICATION SYMPOSIUM

MARCH 6, 2009

HOW A BILL BECOMES A LAW, REALLY

California State Senator Joseph Simitian

At some point in your life you probably opened up a high school civics book to review a flow chart labeled "How a Bill Becomes a Law."

Though complex, the process that chart describes seems relatively thoughtful, deliberate, and in its own way, quite orderly. It is a substantially accurate description of the process in theory, which is to say it bears only a passing resemblance to the process in practice.

In truth, the legislative process is far more random, dramatic, and idiosyncratic than any flow chart could ever describe.

Indeed, Assembly Bill 700, the security breach notification legislation, which is the subject of my remarks this afternoon, is the law today only because of a spelling error, an afterthought, an unrelated concern with digital signatures, a page three news story, the rule of germaneness, the intellectual quirks of a lame-duck Senator, the personal experiences of 120 State legislators, and another bill altogether, Assembly Bill 2297.

That being the case, I've entitled my talk this afternoon "How a Bill Becomes a Law, Really."

In early 2001, I was newly-arrived in Sacramento, a just-elected member of the California State Assembly; and at my request, the then Speaker of the State Assembly created a six-member Select Committee on Privacy, and named me as its Chair.

In that capacity I began to explore the issue of on-line privacy, and met with industry representatives from Silicon Valley, the area I represent. I followed up with academicians and attorneys, as well as consumer advocates and privacy buffs. And I read as much on the subject as my schedule permitted, so that by February of 2002, I was ready to meet with industry representatives again, this time in Sacramento.

Somewhat naïvely, perhaps, I was determined to employ a "different" kind of process in exploring these issues—a conversation and a collaboration, rather than a debate or an adversarial argument. Into a room with perhaps 25 or 30 industry lobbyists and advocates I marched with a "Discussion Document" containing a list of nine issues related to online privacy.

Notwithstanding my repeated assurances that none of these nine items was in fact a formal proposal, the advocates who assembled assumed that none of these items would have been on my agenda absent some interest on my part in pursuing the items legislatively. The result was a meeting, which perhaps inevitably, focused more on defensive posturing than creative collaboration.

In truth, what I was looking for at the time was a relatively narrow issue to pursue; one that was well defined, with high prospects of passage. I thought then, and still do, that on-line visitors needed additional protection, and I held to the view that incremental progress was better than no progress at all.

As the February 22nd legislative deadline for bill introduction drew near, I had narrowed my list of possible proposals to a handful, and was inclined to introduce a bill that would focus on just two very limited but important functions: a requirement that anyone collecting personal identifying information online from Californians be obliged to post a privacy policy, and that they be obliged to comply with that policy (however limited or expansive it might be).

That was it. As I envisioned it at the time, that was the whole bill.

Before I formally introduced the bill, however, I thought it might be helpful if my staff and I checked one last time with a pair of behind-the-scenes advisors—two privacy savvy lawyers who had made themselves available to help on an occasional, and ad hoc, basis.

One was a fellow named Chris Kelly, formerly the Chief Privacy Officer at Excite@Home, and today the Chief Privacy Officer at Facebook. The other ad hoc advisor was a woman named Deirdre Mulligan, who just the year before had joined the Samuelson Clinic here at U.C. Berkeley.

Less than 48 hours before our legislative deadline, we put together an after-hours conference call. I quickly explained the bill, and asked for comment. Both Deirdre and Chris thought it was a good first effort. The bill was narrowly tailored, and modest in scope, but it was a significant privacy "plus" for folks who were doing business online. Yes, it was modest; but it was meaningful progress in a developing area of the law.

And then, almost as a throwaway, I asked "anything else?" "Well," suggested Deirdre, "If you wanted, you could add something else to provide notice in the event of a security breach—unauthorized access to confidential data. I know it's a long shot, but it might be worth a try. And if you actually got it passed, it would be a very big deal."

I hesitated for a moment. Notice of a breach had in fact been among the issues on my original nine item discussion agenda, but I'd passed it by as

overly ambitious. "What do you think?" I asked Chris, who answered, "Sure. Why not give it a try? The push-back will be huge; but if nothing else, it's a bargaining chip—a give-away as you move your bill through the process."

"O.K.," I said. "Let's do it." And in a split second, the decision was made. An eleventh hour afterthought became a part of the bill. One day before the deadline, I introduced Assembly Bill 2297, "The Online Privacy and Disclosure Act of 2002."

And that's when things got interesting because, as it turns out, the bill was a very hard sell—moving off the Assembly floor with just 41 votes (the bare minimum in an 80-member house).

But unbeknownst to me, I was about to catch a break.

According to subsequent press reports, "on April 5, 2002 computer hackers were able to illegally access sensitive financial and personal information, including the Social Security Numbers, of approximately 265,000 State workers, from a State database maintained at the Teale Data Center. According to the California State Controller's office, the information on these computers also contained employees' names and (payroll) deduction information . . . ."

The April 5th breach was apparently not discovered, however, until May 7th, and State employees were not notified until May 21st, nearly a month and a half after the incident. According to testimony heard in the State Senate it was during this time that "unauthorized persons in Germany attempted to access one state worker's bank accounts and another employee had an unauthorized change of address attempt made on her credit card account."

Significantly, among the 265,000 State employees whose data was compromised, there was a 120 member subset of employees critical to our story: eighty members of the California State Assembly and forty members of the State Senate—all of whom received the same form letter, almost two months after the incident, informing them of the breach.

Now, one of those State Senators was Mr. Steve Peace, a twenty-year veteran legislator in the final months of his final term, and not unimportantly, also the Chairman of the Senate Committee on Privacy.

In early June, still 2002, as my A.B. 2297 worked its way through the process, Senator Peace called an informational hearing to explore the ramifications of the incident at the Teale Data Center. Disturbed by what he found, Mr. Peace decided to propose legislation to address the need for notice; but quickly discovered that an existing bill, my own A.B. 2297, was coming his way, which created a bit of a turf problem.

On the Senate side of the Capitol, Mr. Peace had a genuine interest in the issue and by virtue of his position and seniority, he certainly had some standing. On the Assembly side, however, I'd been working on my bill with some success, and notwithstanding my status as a first term member in the Assembly, by the unwritten rules of the Legislature, I legitimately "owned" the issue.

The proposal I received from Mr. Peace, which was relayed by his staff to my staff to me, was that I should drop the "security breach" provision in my bill, that he would 'gut and amend' one of his bills to address the issue, and that I could be named principal co-author of Mr. Peace's bill in the Senate.

I was, to put it succinctly, unenthusiastic about the offer. While I respected Mr. Peace's standing and expertise, not to mention his clout, it seemed to me that I was being asked to be second banana on my own bill; and I suggested an alternative.

"How about I strip the 'security breach' language out of my A.B. 2297, but we both do a gut and amend to create a pair of security breach bills with identical language in the Assembly and the Senate?" On Senator Peace's bill I could be named as his principal co-author, and on my identical bill Senator Peace could be listed as my principal co-author.

In this way we would double our chances of successfully moving a bill through the process, we would both be genuine collaborators as to the content of the bills, and our respective contributions to the field would each be duly recognized. Mr. Peace considered, agreed, and we were on our way.

For my part, since I was still intent on moving A.B. 2297 with its original privacy policy and compliance provisions, I needed another vehicle—a bill that is—that could accommodate a "gut and amend" and become a security breach bill.

Happily, I had A.B. 700, a bill I wasn't using—an altogether unrelated piece of legislation dealing with digital signatures. I had introduced the digital signature bill a year and a half earlier at the behest of the California Association of Realtors, got it passed in the Assembly and then, when the bill proved unnecessary, let it languish in the Senate, where it sat quietly at this point in our story.

Now, in order to amend a bill, the proposed amendments must be "germane." And while "security breach" and "digital signature" issues may strike many of you as more or less unrelated—this was a case of "close enough for government work." Both bills did in fact deal with the conduct of business online; and perhaps more importantly, even as a first term Assembly member, I had already learned that "germaneness" is in the eye of the beholder. It

is essentially whatever forty-one members of the Assembly and twenty-one members of the Senate are willing to let it be. And so it was that A.B. 700, a digital signature bill, which had long been in hibernation, became an active effort at making new law on the issue of breach and notice.

Though the timeline was tight, our twin bills moved swiftly through the system.

The fact that every member of the Legislature had just been a tardily noticed victim was of immeasurable help. The issue was no longer hypothetical; it was now real, and it was personal.

Moreover, the fact that the bill regulated the behavior of State government as well as the private sector put many Republicans more at ease than a business directed bill might have done. For a number of my Republican colleagues, this was a chance to wag a finger at an unresponsive State bureaucracy, and they were happy to take it.

Mr. Peace's standing, staff, and expertise were helpful as well, and it didn't hurt that he was not only Chair of the Senate Committee on Privacy, but also the Chair of the Senate Budget Committee and our bicameral Budget Conference Committee. His bill moved, and so did mine.

As amendments were taken, token opposition become almost nonexistent. On August 31, 2002, the final day of the two-year session, the Assembly concurred in Senate Amendments by a unanimous vote on a special consent calendar, and, without any debate whatsoever, A.B. 700 was on its way to the Governor.

But still, the saga continues. As a pair of identical bills makes their way to the Governor, the obvious question is which one, if either, is about to become law. As it happens, if the Governor signs both bills, the second bill signed either "chapters out," or replaces, the first bill signed; or, at a minimum, supersedes an earlier identical provision.

The author of the second signed bill therefore gets to say that his bill has become State law. The author of the first signed bill, who of course is looking for bragging rights of his own, gets to say that his bill broke new ground and changed state law, if only for a moment.

In such a circumstance, of course, you can't help but wonder, when these two bills hit the Governor's office, in a crush of 1,379 end-of-session bills, will anybody notice, or care, which bills gets signed first. In fact, they do.

It turns out that the Peace bill had a typo, a spelling mistake. The error is noted and reported, so the Peace Bill is signed first, and my bill, A.B. 700, the Simitian bill, is signed second. The expectation then is that my bill will supersede and/or chapter out the Peace bill. Except, as it turns out, the legislation

Mr. Peace and I have authored does not simply amend existing law—it creates a wholly new statute: Sections 1798.29 and 1798.82 of the Civil Code.

That being the case, the duplicate statutes, all but identical except for the typo, both become law, and follow one after another in the Civil Code—almost indistinguishable, except that Mr. Peace's version may be identified by the missing "c" in "acquisition," roughly halfway through the code section.

At least that was the case until January 1, 2008. On that date, the redundant language in the code was corrected by yet another bill—Assembly Bill 1298 by Assembly Member Dave Jones—that made changes to existing law relating to the disclosure of personal information, including medical information maintained by a business or state agency or contained in a credit report. In addition to those substantive changes in law, A.B. 1298 repealed the duplicate sections of law placed into the code by Mr. Peace's bill back in 2002, leaving only the language of A.B. 700.

All of which is neither here nor there. The credit (or the blame, depending on your point of view) is properly shared by each of the two authors—each of whom brought something essential to what was ultimately a successful effort.

That being the case, it's probably time to look more closely at the substance, rather than the saga, of A.B. 700.

The underlying rationale for A.B. 700 is simplicity itself. Before a consumer can protect himself from the unauthorized acquisition and use of confidential information, the consumer has to know that an unauthorized acquisition has occurred.

Without that knowledge, the consumer isn't even aware of the need to protect himself—never mind thinking about the ways in which he might want to protect himself.

Simply put: to be unaware is to be vulnerable. And at its core, that's what A.B. 700 is all about.

By its terms, the bill provides that "any person or business that conducts business in California, and that owns or licenses computerized data that includes personal information, shall disclose any breach of the security of the system . . . to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person."

The same basic requirement applies to someone who maintains such data for an information owner or licensee; and, as mentioned earlier, the provisions of A.B. 700 apply to State agencies, in addition to private entities and individuals who "conduct business" in California.

As the bill worked its way through the system, a number of amendments were incorporated which were designed to respond to the concerns expressed by business and industry.

Among the accommodations to industry:

The notice requirement generally does not require notice of unauthorized acquisition of encrypted data.

The definition of personal information is more limited and narrowly tailored than originally proposed.

A legitimate delay in providing notice is authorized when necessary to accommodate legitimate law enforcement efforts.

The language of the bill was modified to help protect industry from unreasonable consequences where information may have been accessed, but not actually acquired, or where a good faith acquisition or inadvertent disclosure is involved.

The bill specifically provides for state preemption of the issue to ensure that cities, counties, or other public agencies in the State will not be able to impose additional or contradictory requirements.

And perhaps more critical to industry representatives, alternative notice provisions were incorporated, so that if the cost or number of notices required proves unduly burdensome, a range of notice options is authorized.

Finally, the operative date of the measure was delayed six months, from January 1st to July 1st of 2003, in order to provide adequate time for informing and educating the State agencies and the business community as to the obligation to comply and the essential elements of compliance; and in order to provide adequate time for public and private entities to adopt the appropriate practices and policies, and further secure their systems.

In its final form, I think A.B. 700 mostly does what it set out to do: it provides some assurance that when consumers are at risk because of an unauthorized acquisition of personal information, the consumer will know that he is vulnerable, and will thus be equipped to make an informed judgment about what steps, if any, are appropriate to protect himself physically and/or financially.

That, as I've said, was and is the core purpose of A.B. 700. There were other goals as well, however.

Certainly when A.B. 700 was written and passed, I hoped to provide an incentive to those responsible for public and private databases to improve their security (and thus reduce the risk for all of us). I believed then and believe now that "shame and cost" are powerful motivators for improved security.

We also hoped, but were not sure, that non-Californians, consumers around the country, would also be protected to some degree, since as a practical public-relations matter it's difficult to inform only the customers in California when a national database is hacked. As it's turned out, this goal has been more fully realized than we might have hoped.

And, finally, we hoped to prod other states or the federal government into taking meaningful action. As you all know, it is the states and not the federal government that have responded to the challenge.

I think I should say at this point that among my principal interests in pursuing A.B. 700, and related legislation, is a firm belief that the future of e-commerce is directly linked to the public's confidence in online privacy protection and data security.

I am a Silicon Valley legislator. In 2001, the American Electronics Association named me their High-Tech Legislator of the Year. And I am firmly convinced that the growth of e-commerce will be stifled until and unless the public and private sectors, together, address the concerns of the buying public.

It is my strongly held view that enlightened self-interest should have made High Tech an advocate, rather than an adversary, for A.B. 700, and the subsequent legislation it spawned. That is perhaps a discussion for another time.

Having said all that, it's time to talk about the next steps.

The passage of time, and action by more than forty other states, makes it appropriate to ask and answer some obvious questions:

How well has the California statute performed during the past six years?

Can it be improved upon, and, if so, how?

And, of course, what have other states been doing; and, what can we learn from them?

My own view after a half dozen years is that there are least two explicit improvements to the California statute that are called for.

First, greater clarity and specificity as to the content of security breach notices is long past due. Our experience tells us that while many of the breach notices sent out may be clear and comprehensive, a substantial number are not—leaving consumers more confused than informed.

Moreover, greater clarity and specificity about the required content of a security breach notification will also benefit businesses and public agencies who presently wonder just what information they need to supply in order to comply with the law.

Fortunately, nearly a dozen other states have already legislated such content standards, and their work can inform our efforts.

The other relatively modest but significant improvement that can and should be made is a requirement that when notice is sent, a duplicate notice should be sent to the state. This simple additional requirement would give law enforcement, state legislatures, and security professionals a better understanding of the nature and scope of the problem and, I would hope, improve law enforcement, legislative action, and security efforts in this arena.

These two improvements are in fact contained in the currently pending California Senate Bill 20, of which I am the author. My hope is that by year's end S.B. 20 will have been passed by the Legislature and signed by the Governor. In my view, that would make a good law, a groundbreaking law, even better.

In closing, I must tell you that my work in this area has been both challenging and gratifying. One of the most satisfying aspects of my work is the opportunity it affords me to explore whole new areas of thought, commerce, or society—or, to put is less grandiosely, to stick my nose into other people's business.

I entered the Legislature in the year 2000 with no background whatsoever in privacy issues, and no real plan or expectation that privacy issues would ever be a part of my legislative agenda.

In 2003, when Senator Peace and I were recognized by *Scientific American* magazine as one of Scientific American's 50 Leaders in Technology, I recalled that my high school science teacher said he always thought I'd be lucky if I could get a paid subscription to *Scientific American*, never mind get myself inside the magazine.

And while I was flattered to be the 2007 recipient of the RSA Conference Award for Excellence in Public Policy, presented in front of several thousand computer security specialists, I must tell you the staff in my office who help me manage my email were more than a little amused.

But I have learned a lot since my earliest forays into the challenging world of online privacy, and if sharing some portion of what I've learned with you today has been either helpful or enjoyable then I'll be very pleased.

But please know how much I appreciate the opportunity to learn from you and how valuable it is for me as a policymaker to be able to tap into your experience and expertise as I go about my business.

I appreciate it. I appreciate your time and attention. And I appreciate the opportunity to share my thoughts with you this afternoon.

Many, many thanks.