July 16, 2006

PRIVACY: American Constitution Society

Thank you very much, Paul. It's wonderful to be here this morning, and I greatly appreciate the opportunity to come before you and speak on a topic that is timely every day, once again today, namely privacy rights. It is a little bit daunting to be introduced by one of the great practitioners of privacy rights law as Paul is.

That depth of expertise that ACS now represents is a big part of the success of this organization – from Paul to your executive director, Lisa Brown– to your founder Peter Rubin, that are part of this movement. Since I spoke at your founding convention three years ago, ACS has grown exponentially. You are filling an unmet need – for a rigorous legal approach that is true at its core to the values of human dignity, individual liberties, and access to justice on which our nation is founded. And your Constitution in the 21st Century project, from Harold Koh on torture to Pamela Karlan on the Voting Rights Act, is doing great work. I want to thank all of you for everything you are doing – and urge you to keep making your voices heard in every way you can.

I am giving a speech today on one of the most important issues facing us today as individuals and as a nation. I believe we are a country headed in the wrong direction in many ways and that it is time to take some fundamental changes in direction in order to make our economy work for people, to protect our national security in a realistic way and preserve our values.

Privacy is at the crossroads of all these issues, and modern life makes many things easier… and many things easier to know. And yet, privacy is somehow caught in the crosshairs of these changes.

Our economy is increasingly data driven. We have dramatically ramped up surveillance in our efforts to fight terrorists who hide among innocent civilians.

But every day the news contains a story of how the records of millions of consumers, veterans, patients have been compromised.

At all levels, the privacy protections for ordinary citizens are broken, inadequate and out of date.

Back when I was in law school- the dark ages- that's actually what our Dean at the time called it… The first thing we learned about the right to privacy was that it sprung from the mind of Louis Brandeis, beginning with a law review article in the 1890s and later in the famous Olmstead dissent that first set out what later courts have recognized as our constitutional right to privacy. Justice Brandeis, as I'm sure you all recall, wrote that the Framers "recognized the significance of man's spiritual nature, of his feelings and of his intellect. . . . They sought to protect Americans in their beliefs, their thoughts, their emotions and their sensations." As Brandeis put it, the Constitution confers "the right to be let alone—the most comprehensive of rights and the right most valued by civilized men: the right to be let alone." Now I can imagine some of you thinking what on earth would I know about that? I'm sure you might find it slightly ironic for me to have chosen the topic of privacy for this talk, since I seem to have had so little of it in my own life.

Now, my experiences with privacy policy have been, let's say, unique. I'm not the

victim of identity theft; though I do sometimes see myself referred to in the media and wonder who they're talking about. But having lost so much of my own privacy in recent years, I have a deep appreciation of its value – and a firm a commitment to protecting it for all the rest you. And, I hope that you take these remakes with that thought in mind, since I am an expert in the perils of losing your privacy.

Most people cherish their privacy – that fundamental desire to be left alone. They see it as essential to their liberty that they be able to go about their daily business free from surveillance and interference. And yet, in modern society – without greater safeguards – we're all open books to whoever has access to the data we create every day, from credit cards to store cameras to phone company records. The challenge we face is how to take advantage of all the advantages of technology without losing something precious – which is I think the challenge that we confront individually and as a society.

Now fortunately, we have a uniquely American way to think about the privacy challenges we face. It is as old as our Constitution and as new as the firewalls on the Internet. It's called checks and balances. Now, that has a specific Constitutional meaning to all of you in this room today, but it also has a broader colloquial meaning that is part of the genius of American society – our ability to balance and safeguard our cherished values even as we take full advantage of new innovations.

I believe it is not just a possibility, but a necessity, that we preserve our right to privacy, while we also participate freely in the modern world and defend our national security.

But if we keep going as we are, there will be little left of that cherished right. Every phone call, every Internet search, every credit card purchase – they are all under potential surveillance from business and government, unless we start to draw the line, reinforce people's basic rights, and put checks and balances back into our system.

Now, privacy and national security have gone hand in hand since America's beginnings. When the Framers adopted the Fourth Amendment, they had in mind the intrusive and threatening searches that British authorities felt free to carry out on a whim. Well, we're reminded of that again today with the Supreme Court's decision. The value of the 4th amendment is as strong and as important now as it was when British soldiers were garrisoned involuntarily in people's homes. The 1967 Katz decision demonstrated how this right evolved with technology establishing a right to privacy respecting wiretaps to the 2001 opinion by Justice Scalia prohibiting the police from using a thermal imager to scan a home without a warrant. Privacy is not and should not be a liberal value or a conservative value. It fundamentally an American value; it is a human value.

Privacy means security in our homes and in our private communications and activities. It is synonymous with liberty, in the sense that every person enjoys a zone of freedom that government may not violate. And we have to operate from a presumption that the Fourth Amendment means that no matter how easily our privacy can be violated, that we still have a basic right to protect the collection and dissemination of information about ourselves from our government. We have to remember that we also have to start all analysis of privacy with this basic notion – individuals have a right to privacy unless there is a compelling reason to breach it. But privacy is not to be the exception, it is the standard.

Today our privacy comes into uncertain conflict with security cameras, data mining, computer hackers and identity theft. We're concerned not just with government actions, but with the ability of the private sector – even our neighbors – to misuse, or provide insufficient protection for, our personal information.

Therefore, we do need legal protections that are up to date with the technological and national security needs of our time – for a world in which we can be confident that our security and our privacy are both protected. And that's what I would like to propose today.

Well right now, many Americans are frightened and confused about losing their

privacy. We see patterns of carelessness and outright fraud at the same time as we are exposed to data-gathering and marketing gimmicks at every turn.

According to the non-profit Privacy Rights Clearinghouse, the personal information of more than one in four Americans – 85 million people – has been compromised in just the last 15 months. Now, some of these were massive breaches, like the theft of a single Veterans' Administration laptop with the social security numbers and medical information of 26.5 million people.

Just this year in my state of New York, an armed robbery in New Jersey netted private information on 17,000 patients from a New York hospital; a hacker broke into a retail website in Buffalo and stole credit card data; data tapes for virtually every employee of the Long Island Railroad were lost by a delivery service; two laptops full of employee data were stolen from Verizon; a hard drive containing information on 300,000 certified public accountants was lost in shipment; a laptop with bank account information was stolen from a subcontractor in Buffalo. Now, that's more than half a million people affected in less than six months in one state.

And the personal stories can be heartbreaking. My office has heard from a minister harassed, wrongly, by credit agencies; a woman whose trusted tax adviser opened bank accounts and stole money in her name; a breast cancer patient whose mammography records were lost.

But at the same time, Americans are asking, privacy at what price, when we are confronted by criminals and terrorists who respect none of our core values. Terrorists don't hesitate to use modern information technology – cell phones and the Internet. We need to be able to track them. Meanwhile, new techniques like data mining have changed many of the things we thought we knew about surveillance. Americans are genuinely unsure about whether we can keep both our privacy and our security.

But this is one of the most fundamental questions about what kind of country we will be. How we greet the challenges of a more connected, data driven world, like our own, while preserving our core values. It's time to take a new comprehensive look at privacy. That's why I am proposing a comprehensive privacy agenda: I'm proposing we have a new privacy Bill of Rights that secures the interests of consumers; provides stronger, better-enforced protection for medical privacy; and a new national security consensus setting out clear rules to allow the government to use new intelligence techniques within a rule of law framework and making sure that the public knows its rights and the government's limits.

When we talk about privacy, we can talk about where most people live – which of us consumer privacy. Few of us would choose to go back to the days where we made all our purchases with cash, and we could only get cash out of the bank during what used to be called "bankers' hours."

In fact, information technology often makes us and our personal information safer. We don't have to carry large amounts of cash around. We can pay bills electronically rather than by mail. But the public doesn't feel more secure – and, with stories like ChoicePoint, or BankAmerica or the VA a thefts in the news, they have good reason not to.

So we need a new set of consumer protections that boil down to three basic rights:

First, people have the right to know, and to correct, information which is being kept about them.

Second, people have the right to know what is happening to their personal information when they are cooperating with a business and to make decisions about how their information is used.

And third, in a democracy, people have the right and the obligation to hold their government and the private sector to the highest standards of care with the information they gather.

These rights should be basic to all of the commercial transactions we undertake and be part of a basic privacy bill of rights that has to be adhered to by every commercial information gatherer or marketer.

email zip GO

My privacy bill of rights will be encapsulated in the PROTECT Act, which stands for – you know when you're in the Congress you have to find acronyms; you spend hours trying to find legislation in words that can eventually spell something, so I give my staff full credit for this – but The PROTECT Act, Privacy Rights and Oversight for Electronic and Commercial Transactions Act. Pretty good, huh? This legislation not only provides clear privacy rules, it gives you clear protections for your most private information, the right to sue when those rules have been violated, the right to protect your phone records, the right to freeze your credit when your identity has been stolen, the right to know what businesses are doing with your credit and credit reports, and the right to expect the government to use the best privacy practices itself with your information.

We should start with the principle that, for the most deeply personal information about how we spend money on a daily basis, your information should be shared only when you "opt-in." We know that a booming industry is tracking every purchase you've made with your debit or credit cards or personal checks. This means that if you've failed to check that tiny little opt out box on your credit card company's or your bank's privacy statement, there may be a profile on what you read, what you wear – and what size – what over the counter drugs you take and what books and music you buy. And that profile then may be bought and sold and shared with third parties everyday.

The opt out protections under current law can be helpful, but for some things the default privacy agreement should be that companies cannot share this information without your explicit agreement to "opt in". Opt out protections essentially assign property rights for your personal information to financial institutions, while opt-in awards ownership to consumers. I believe applying opting in for these types of transactions would reinforce the relatively simple and reasonable concept, that you own your information about yourself and you should have control when, how, or if it is shared.

The foundation of our legal system is the right to seek redress through the courts. Right now, we have no set definitions of what privacy violations cost the individual and little incentive for banks and other businesses in many instances to protect your data with the highest level of security. As a result it is very hard for consumers to sue. Legislation I'll introduce will create a tiered system of damages, exempting the smallest businesses with set minimums of $1000 for breaches and $5000 for actual misuse of information.

The burden of prevention belongs on the companies that handle our data. We established this principle for stolen credit cards in the 1968 Truth in Lending Act – and that has spawned a whole industry of credit card protection, which is constantly improving to outwit thieves. We need the same standards for other information.

Right now the rules covering data processors are unclear, especially in cases where projects are outsourced. We need the FTC to issue a single, clear set of rules that provides comprehensive protection against unauthorized access or security breaches.

Right now, it's too easy to purchase, post or trade cell phone numbers and records. Canadian government officials, journalists, even General Wes Clark, have had their cell phone numbers and records sold to anyone willing to put up the money. And those are just the cases we know about, because reporters and bloggers were doing the buying to draw attention to the threat. Buying and selling that kind of information is a gross invasion of personal privacy – but it's not clear that it is a crime. And this is only going to get more challenging as consumers move to phone service based on broadband Internet technology for which no regulations currently exist.

My legislation will try to get ahead of the curve of technology, making sure that consumers' private cell phone numbers and call records remain private.

Right now, if you've been victimized, you can place a credit alert. But you cannot freeze your credit. If you are a veteran, concerned about your credit because your Social Security Number has been compromised, you should be able to call Equifax and say, "No access, and no new credit."

We also have to strengthen the right to know provisions. If your credit or identity is compromised, you should be notified immediately not days, weeks, even months later. Because this is required in some states but not all, a large percentage of identity theft victims are unaware that anything has happened to put their information at risk.

Some firms are now sending data abroad for processing, away from the protections of U.S. law as inadequate as it is – at least it has a framework better than you'll find in the rest of the world. The potential dangers of this practice are illustrated by the case of an employee in a Pakistani data center doing cut-rate clerical work for an American medical center, who threatened to post patients confidential files on the internet unless she was paid more money. Moreover, last year employees doing data processing work for an Indian outsourcing company stole $350,000 from four Citibank customers. Last year, I proposed the SAFE-ID bill which ensures that consumers will be notified when their personal data is sent abroad, and they should have the right to opt out.

This would have two benefits. Again, putting the control of information in your own hands. But also sending a message to other countries if they want to continue employing people in this very lucrative, rapidly growing area of information handling they need to strengthen their own laws.

The credit industry makes its profits from information that determines whether you can buy a home or send your child to college. You ought to have that information provided to you once each year without paying a fee or jumping through hoops. It shouldn't be a gold-plated, extra-fee service to let consumers know when someone changes their credit ratings – and we need to make that standard practice.

Across the federal government, privacy concerns are not getting the priority attention they deserve. The results are embarrassing to this Administration and unacceptable for citizens whose privacy and security may be at risk from their own government's sloppy practices. That's why the PROTECT Act would create a high-level privacy czar in the Office of Management and Budget. A Chief Privacy Officer for our government would have oversight into the workings of every government department, and power to make sure that the law is being followed and best practices are being implemented. We had a privacy czar during the Clinton Administration, but the current administration chose not to follow that model.

There's no better example of why we need a so-called Privacy Czar than the theft last month of personal data from those 26.5 million veterans and more than a million active-duty servicemen and women. And just yesterday, we learned that an offshore medical transcription subcontractor for the VA threatened to post the medical histories and health information of over 30,000 veterans online over a payment dispute. This tells us that the oversight of data processing procedures at the management level of our federal agencies is insufficient at best since several VA officials including the director were not even aware that their contractors were sending the most sensitive information of our veterans to countries with few privacy and data security regulations. It's part of the reason we need the SAFE-ID protections I mentioned earlier. But we need to go farther.

This week I joined with Democratic colleagues to demand accountability from the administration for this personal data theft of millions of records. We are asking the U.S. Comptroller General to conduct an in-depth study to get the facts on this breach and to address the vulnerabilities that led to it. We also introduced legislation to establish Federal penalties for people who knowingly use personal or health information from a Federal database. The theft of this data and the Administration's lax response is a disgrace – soldiers serving in harms' way should not have to bear the additional burden of worrying about identity theft, and we need to get to the bottom of this to prevent it from happening again. Perhaps, if we had the Office of the Chief the Privacy Officer, this breach of our service members' trust might not have happened or come to light much sooner.

We also face a critical balancing act in the area of health privacy. Patients' lives may depend on sharing their most intimate information. Our ability to control costs and

improve the quality of healthcare certainly depends on moving away from paper-based medicine to information superhighway medicine.

email zip GO

I've worked with Newt Gingrich on this, and when Newt and I agree, you know something unusual is happening.

Newt likes to say, when it comes to medicine, "paper kills," and he's absolutely right. But if we can't assure Americans that their information is safe, we won't be able to move forward on health information technology that I believe will save lives, improve care, and reduce error rates.

We had no federal protections for health information at all, until the Health Insurance Portability and Accountability Act – also known as HIPAA, a different kind of acronym – was enacted under the Clinton Administration. HIPAA provided important protections of patients' often most private information – their medical information. HIPAA provides a baseline, but the business of healthcare is changing fast, and information technology is changing even faster. Consumers are getting care and risking their information in ways nobody could have foreseen years ago; and frankly, this administration's indifference towards HIPAA and enforcement has made even the protections we have utterly inadequate.

Now, HIPAA is not without practical challenges – there is still confusion about the rules for releasing information to relatives for example. We are still trying to strike the right balance between promoting research into diseases and protecting an individual's information. We need to build on the base HIPAA provides by improving enforcement and making sure we have one set of high standards for everyone who deals with health information.

HIPAA was designed to have teeth – government monitoring, fines and legal actions against companies that violate the law. But instead of spot checks and audits, HHS waits for a complaint and then investigates. There have been well over I think 35,000 complaints at the last count and not a single civil monetary penalty has been imposed. This is clearly not working. And because of lax enforcement, we're now seeing compliance with HIPAA on the decline because people know they won't be held responsible.

What is more, the Department of Justice ruled last year that employees of HIPAA-covered entities, like hospitals for example, are not themselves automatically liable, and therefore may not be held accountable for illegally accessing or misusing private information. And hackers who break into computer systems that are covered in institutions that are accountable to HIPAA may also not be liable.

Now, this penalizes those businesses that are serious about protecting privacy – and it penalizes Americans when they are most vulnerable. We need to get back into balance on protecting medical information and enforcing the rules we do have.

Now, consumers have all kinds of new on-line options in healthcare. They can go to sites like WebMD for medical advice. They can create Internet-based personal health records that keep all their information in one place. But HIPAA doesn't protect you, if these new services violate their privacy. We need to strengthen the federal protections so there is no debate – everyone who traffics in your health care information is accountable. Period. No exceptions.

With the rapid growth of DNA databases, and the many uses of genetic information on the horizon, we must also ensure that this information is protected to prevent genetic discrimination. In 2000, my husband issued an executive order banning genetic discrimination in the Federal workplace. I have been working with my colleagues in the Senate to enact legislation to ensure that these protections apply to the private sector. Developments in science should move us forward, not reverse progress. And discrimination based on genetic information to get a job, to get insurance would be a devastating blow to people if this is left unchecked.

Finally, when it comes to national security. We've seen, to our dismay, that this Administration is not doing a good enough job of protecting the personal information of veterans, Medicare and Medicaid patients and we have grave doubts about whether it even cares to protect personal information about citizens.

email zip GO

We learned just a couple of days ago that in September of last year, a computer hacker was able to steal the personal records of at least 1,500 employees and contractors of the National Nuclear Safety Administration, that is the federal agency charged with guarding out country's nuclear weapon stockpile. This time it was personal information. Next time who knows what kind of information will be compromised or how either forms of information will be used. The writing is on the wall – it is in neon – it is time to get serious about cyber-security.

Unfortunately, the task of beefing up our cyber-security has been kicked around multiple offices at the Department of Homeland Security. Several political appointees have quit in frustration. We are just living on borrowed time; we need to make sure that we are better-prepared against cyber-attacks than we turned out to be against hurricanes.

We also face the challenge of balancing the vital role that information technology plays in defending our national security with our citizens' rights to privacy.

So much of what we know about terrorists, and the successes we have had in preventing and thwarting attacks and tracking would-be perpetrators, has been through information technology. We track terrorists across continents through their cell phones. We monitor terrorists and their supporters through Internet chat rooms. We had phone intercepts that should have given us advance notice of 9-11 if we had been paying attention.

Now although our Founders couldn't imagine data mining or terror cells, they did anticipate differences of opinion between the executive and legislative branches, and even within them. And they created the system of checks and balances enshrined in our Constitution.

Now I believe that the President – and I mean any President – must have the ability to pursue terrorists and defend our national security with the best technology at hand. But we have existing law that allows that – the Foreign Intelligence Surveillance Act or so-called FISA. We have judicial mechanisms in place that this Administration could have used to obtain authority for what it did; we have a system of Congressional oversight and review that this Administration could have used to obtain a legislative solution to these challenges.

Instead, they relied on questionable legal authority and bypassed our system of checks and balances. In the months since NSA's activities have come to light, both the legislative branch and the judiciary have attempted to learn more about the Administration's surveillance programs. In denying Congress and the courts any information, the Administration's refrain has been "Trust us." They've used it to justify frustrating legislative oversight, denying the Department of Justice's Office of Professional Responsibility the clearances they needed to conduct an internal investigation, and just a few days ago we learned they are now invoking the State Secret Exception to shut down any judicial review of their conduct through assertion of that privilege. That's unacceptable; their track record does not warrant our trust.

This has been the point of numerous decisions, not on this point exactly, going back several years.

And in Justice Douglas' concurrence in the Katz warrantless wiretapping case in 1967, he said it very clearly and I think it applies today: "Neither the President nor the Attorney General is a magistrate. In matters where they believe national security may be involved they are not detached, disinterested, and neutral as a court or magistrate must be. Under the separation of powers created by the Constitution, the Executive Branch is not supposed to be neutral and disinterested. I cannot agree that where spies and saboteurs are involved adequate protection of Fourth Amendment rights is assured when the President and Attorney General assume both the position of adversary-and prosecutor and disinterested, neutral magistrate."

The answer to this delicate security dilemma is neither blank checks nor blanket opposition; it is to use the judicial and legislative mechanisms we have to build a consensus about what is necessary, what is legal, and what is effective.

So first, Congress must have an oversight role and help decide where to draw the line

between privacy and national security. But we can't draw anything without knowing the facts. At a minimum, the House and Senate Intelligence and Judiciary Committees are entitled to know, on a confidential basis whenever and wherever necessary, the full extent of and rationale for any electronic surveillance programs.

If the executive needs additional authority to legitimately monitor and track terrorists, it should not just simply overlook and ignore the law. If the President feels he needs to more flexibility in order to protect our security, he should engage the Congress. As our technology and methods become more advanced and creative, so should the protections we build into our system of checks and balances. It is a cause for deep concern that the Administration did not seek changes to the FISA law to legitimize its surveillance program but instead deliberately chose to act outside of that law.

Second, the judiciary has a critical role to play in guarding our privacy from unnecessary government intrusion. As a general rule, when the government wants to conduct electronic surveillance in the United States, it must go before a judge and obtain a warrant. There is no evidence that the courts have not taken seriously the national security imperatives asserted by the Executive Branch and effectively protected the security of sensitive information. The FISA courts have a proven track record of being able to protect our security and privacy simultaneously. We can allow for carefully defined exceptions to the warrant requirement in the immediate aftermath of war, and allowances can be made for greater flexibility. For example, warrants after the fact, in cases of true emergencies. But as Justice Harlan said in the Katz case, "warrants are the general rule."

Third, any framework for domestic surveillance must ultimately facilitate not hinder, effective intelligence-gathering to prevent terrorism. Our surveillance capabilities must have speed, agility, and flexibility. They must also be accurate – both to minimize false positives, which unduly burden the rights of innocent people, and false negatives, which leave potential dangers undetected. This can all be done within our system of checks and balances and within the rule of law.

The rule of law is not an obstacle – despite what some in the executive branch seem to believe – in fact, the rule of law facilitates our safety and our security. Without clear rules, our intelligence analysts don't have guidance on how they should gather intelligence; the intelligence they do collect is distributed haphazardly throughout government agencies; and useful intelligence that could help bring terrorists to justice could be rendered worthless, because it was gathered through extra-legal means. If we want to protect our security and our privacy, we need clear guidelines and to we need to get smart about technologies. One promising approach suggested by thinkers on both sides of the political spectrum is the use of anonymization - that's technology that protects the privacy of individuals while allowing the government to analyze data. This technology would essentially erase the personal identification attached to information that is monitored, unless red flags are triggered. Whatever our approach, we need to be as creative and imaginative in protecting Americans' privacy as we are in protecting our security. And we need to abandon the idea that privacy and security are somehow mutually exclusive.

You know, in our society it is the people who have given their collective rights to the government to use only as necessary – the government derives its ability to undertake surveillance only because we have given it a limited right under justified circumstances.

And you don't have to go back many years to document abuses at the highest levels – as a very young lawyer, I worked for the House Judiciary Committee during the Watergate Investigation. Our Committee found the President had not only bugged the Democratic National Committee with former CIA operatives, but had also created enemies lists and manipulated IRS audits. Without the rights checks and balances, we found out just how quickly the unthinkable can be done by people whose power is unchecked.

Now as there is a legitimate rush to step up our intelligence for real needs, let's not forget all the lessons we've learned over the past 220 years. What might seem sensible at the moment can be used unscrupulously in the future. Unchecked mass

surveillance without judicial review may sometimes be legal but it is dangerous.

Every president should save those powers for limited, critical situations. And when it comes to a regular program of searching for information that touches the privacy of ordinary Americans, those programs need to be monitored and reviewed as set out by Congress in cooperation with judiciary. That is the essence of the compact we have with each other and with our government, and we cannot ignore it.

So we don't need to abandon our cherished rights. We don't need more false debates— liberty vs. security, privacy vs. danger. What we need is to come together and develop a consensus on how to protect our privacy in a more data driven and more dangerous world. This issue is too important to be dealt with haphazardly, and it is really too important to be ignored. So let's stand by a few cherished American ideals; let's think intelligently about how they apply about what we face in the new century within the framework of values that have stood the test of time.

We are after all country built on individual liberty, including individual privacy, as well as collective safety and security. We have been very good over the years in resolving the tensions between those two points. And as we look at the rights of the people and the imperative of government we need to see them through the same vantage point, not as competition, but as all of seeking the kind of results that will make us a safer, freer people. Our Constitution is fully up to the challenge of protecting our privacy and our security today. The question is whether we are up to the challenge of enacting laws and implementing policies that honor it.